PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : A61B 5/117

A1

(11) International Publication Number: WO 00/13588

(43) International Publication Date: 16 March 2000 (16.03.00)

(21) International Application Number: PCT/US99/20373

(22) International Filing Date: 3 September 1999 (03.09.99)

(30) Priority Data:
09/148,914 4 September 1998 (04.09.98) US

(71)(72) Applicant and Inventor: BEECHAM, James, E. [US/US]; 8820 Cortile Drive, Las Vegas, NV 89134 (US).

(74) Agents: FLIEGEL, Frederick, M. et al.; Wells, St. John, Roberts, Gregory & Matkin, P.S., Suite 1300, 601 W. First Avenue, Spokane, WA 99201-3828 (US).

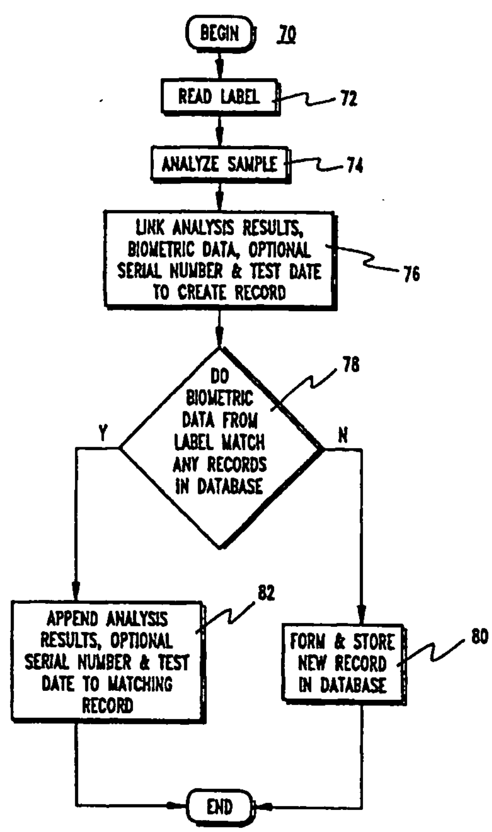
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: VERIFICATION OF HUMAN MEDICAL DATA

(57) Abstract

Methods and apparatus for correlating blood, tissue samples or donor suitability with a donor or recipient while optionally preserving anonymity for the prospective donor are described. One method may include steps of collecting a blood sample (14) from the donor and taking biometric data (37) from the donor. The biometric data permit a high order of probability of correlation of the donor with the blood sample (14) and with test results derived from the blood sample. The method optionally further includes a step of providing the donor with a unique correlating code also for permitting unique correlation of the donor with the blood sample and with test results derived from the blood sample and may further optionally include a step of labeling the blood sample (14) with information including the biometric data (37).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

DESCRIPTION

VERIFICATION OF HUMAN MEDICAL DATA

Cross-Reference to Related Applications

This application is a continuation-in-part of U.S. Patent Application Serial No. 08/910,062, filed on August 6, 1997, which is a continuation-in-part of U.S. Patent Application Serial No. 08/686,211, filed on July 23, 1996, which are both owned by the same entity as the instant application.

Technical Field

The instant invention concerns methods and apparatus for voluntarily providing medical data for humans and allowing a donor to uniquely identify blood or organs donated by that donor or another donor.

Background Art

Examples of medical data collection, storage and display systems are described in U.S. Patent No. 4,737,912, entitled "Medical Image Filing Apparatus," issued to Ichikawa and in U.S. Patent No. 5,193,541, entitled "Health Examination Method And System Using Plural Self-Test Stations And a Magnetic Card," issued to Hatsuwi. This patent describes a system for storing medical data on magnetic media contained on a card. The patient provides samples and the like to a variety of testing stations that also record self-test data on the card.

A further example is taught in U.S. Patent No. 5,325,294, entitled "Medical Privacy System," issued to Keene. This patent describes a system and method for retrieving medical data from a database and sharing these medical data voluntarily with another party while protecting against access by unauthorized parties.

A feature common to such systems is a means for identifying a particular patient or client and associated medica records. Areas where such concerns arise are: (i) blood sample collection/donation, (ii) testing to determine human health characteristics, including infectious status of humans, and especially HIV status, and (iii) organ donation following the brain death of a suitable organ donor.

Blood samples may be collected for various purposes, including blood typing, drug testing, testing for infectious or genetic diseases, blood donation and organ harvesting. Depending on the purpose of the donation, various specific blood specimens may be collected. For example, a patient may donate blood for autologous transfusion in anticipation of elective surgery, *e.g.*, hip replacement. The autologous donor is also the intended recipient of the donated blood. The patient donates blood over a period

of weeks, and the donated blood is replaced by the patient's bone marrow in the normal manner. In this way, the blood lost during surgery may be replaced with the patient's own blood, which was stored in a blood bank from the time of donation until the surgery.

Another situation in which quasi autologous blood donation occurs is in the context of a woman giving birth to a newborn child. The umbilicus and the placenta includes substantial quantities of blood that is laden with unique cells and substances believed to be efficacious in promoting healing and particularly in treating childhood leukemia. A growing number of women giving birth are electing to have the blood drawn from the umbilical cord and placenta following the birth, and to have this blood stored in a blood bank. The stored blood, known as "cord blood," is then available for the infant in the event that the infant requires surgery or has other need for a blood transfusion, and in particular if the infant should develop a need to regenerate bone marrow. In this case, the identification on the blood sample should not be only that of the birth mother, because the birth mother may give birth to or have previously given birth to one or more other children.

As with most specimens for laboratory testing, it is desirable to have a way of linking the specimen to the donor from which the specimen was collected. In autologous blood donation, identification linking the donor to the donated blood is critical, particularly when the patient has a blood-borne disease, *e.g.*, is hepatitis B or HIV positive. This linked identification is needed in order to ensure that the blood being transfused at the time of surgery was donated by the patient undergoing the surgery. Typically, the name of the donor and other identifying indicia are written by hand on a label (or, alternatively, a computer-generated label is prepared including the linking data) and the label is affixed by adhesive sticker to the sample collection receptacle side wall.

This label is attached to the receptacle side wall either after or before sample donation. Thus, prior to attachment or recording of data, the label can be inadvertently transferred with another label and affixed to another receptacle, or the data may be recorded on the wrong label, incorrectly placing the name of one patient onto a receptacle holding a sample from a different patient. This may result in erroneously reported lab results leading to improper diagnosis and treatment of the patient or improper identification of one individual as having used some drug or substance or transfusion of the wrong type of blood to a patient.

In some other settings, blood for transfusion to humans is selected based on compatibility testing. Typically, a medical technologies performs a crossmatch using a blood sample from the prospective recipient and a sample from a donated unit of blood. Testing both samples verifies that no antibodies or hemolytic agents are present in the recipient that would react against the cells in the donated unit to produce lysis of the donated red blood cells when transfused into the recipient. Several commercially available labeling systems are known whereby a unique number or bar code label can be attached to the sample blood tube holding blood collected from the prospective recipient, to the wrist band of the prospective recipient and to another label having the identical alphanumeric or bar code to be attached to the receptacle holding the crossmatch compatible donated blood unit. The label may state that testing has confirmed that the unit is compatible for transfusion to the crossmatch compatible recipient. The medical personnel tasked to administer the transfusion will thus be able to compare the number appearing on the crossmatch compatible donated blood unit container to the number on the prospective recipient wrist band and thus to administer the correct crossmatch compatible blood to the corresponding correct recipient. In a similar manner, the prospective recipient's name can be included on the wrist band attached to the recipient, and on the blood tube representing the phlebotomy sample collected from the prospective recipient. The label is usable for sample identification during crossmatch testing in the laboratory. The prospective recipient's name can appear on the label of the blood unit when such blood unit is verified as crossmatch compatible by the medical technologies in the crossmatch testing.

Limitations occur with the above-described systems, in particular where the medical personnel collecting the sample of blood from the prospective recipient inadvertently place the wrong label on a phlebotomy sample tube. The phlebotomy sample tube then bears a label having the name or number from another patient rather than the name/number of the true patient source of the phlebotomy blood sample. This happens, for example, during situations in the emergency room wherein a phlebotomist is performing phlebotomy on several patients in a row. The phlebotomist may label two tubes prior to drawing blood from two patients and by error place blood drawn from patient A into the tube labeled with the name and associated number from patient B. The resulting transfusion of blood crossmatch compatible for patient A into patient B, in some cases, leads to a serious blood incompatibility reaction occurring in patient B which may have serious adverse consequences for the health of patient B.

Another potential source of error involves the process of hanging a unit of blood at bedside whereby the nurse takes the unit or donated blood from the blood bank to a patient. Prior to infusing the blood, the nurse checks the wrist band to verify that the name and number on the container bag of blood for transfusion. This identification is not always carried out properly. For example, the nurse may only go the chart rack and check that the patient for whom the order is written is in a certain bed number. Then the nurse will go to that room and transfuse the blood into the patient occupying that bed regardless of the fact that on occasion someone on the previous nursing shift may have reassigned beds and moved the true intended recipient to another bed. Moreover, patients have been known to exchange wristbands or alternatively wristbands may be cut off while IVs are placed into wrist veins or during surgery where such wristbands are often then taped to the front of the chart, sometimes the wrong patient's chart.

Similarly, where the nurse only asks the patient his or her name verbally rather than checking the wristband, there are known to be errors. For example, a patient may not be fully functional in hearing or language and may respond inappropriately. Where the nurse has several patients needing transfusion and inadvertently takes a unit of blood intended for patient C to the bedside of patient D and then incorrectly omits reviewing the wristband data, or in reviewing the wristband data does not detect a difference in number or name where similar family names are present (as in an accident hospitalizing several family members together), then that nurse may inadvertently transfuse blood intended for patient C into patient D, resulting in a transfusion reaction in patient D.

In order to maintain a blood supply, blood banks solicit donors who donate blood. Typically, donors of blood units are first screened by the blood bank staff asking the prospective donor certain pertinent questions, *i.e.*, taking a medical history and performing medical tests such as blood pressure, hematocrit, etc. Among these questions are those designed to identify high risk behavior such as men who have sex with men, drug abuse (especially intravenous), tattoos, history of hepatitis, medications, etc. These questions are dsigned to protect both the donor and the recipient. For example, certain high risk behavior is known to be associated with a greater risk of infectious disease in the donated unit.

Where a donor is deferred, *i.e.*, not permitted to donate blood at one blood center, that donor may attempt to donate at another blood center. This is a risk for the blood supply since donor deferral for high risk behavior or positive test markers is

important to reduce the chance that the blood unit for transfusion might carry an infectious agent.

Although most donors are voluntary, some are paid, as for example in some centers collecting blood-derived fluids such as plasma donation centers. This economic aspect further increases the need to screen and defer donors unsuitable for donation.

Some donors deferred at one center may appear with the intent to donate at another blood donation center and try to conceal the previous deferral and the reasons for this deferral. In some cases, the deferred donor may not be truthful in answering questions at the second blood donation center, i.e., in the circumstance where the donor wishes to have a test for HIV done by the blood center rather than admit to engaging in high risk behavior. In this circumstance, the blood donation center needs a system that specifically identifies a deferred donor, i.e., one deferred by another blood donation center.

In all of these examples, samples of blood are typically collected by puncturing the skin and removing a sample of whole blood by vacuum or by the blood pressure in the donor's artery or vein, as is explained in more detail below. A tourniquet is typically applied to the arm, or in some cases, the leg, of the donor and the skin surface is swabbed with alcohol to disinfect it. Subsequently, the donor is often asked to grip a rubber grip so that the natural muscle compression leading to blood flow in the venous system is utilized to cause the vein to engorge and swell indicating that blood volume has increased in the vein. Then a needle attached to a syringe is inserted into the vein and a quantity of blood is removed. Alternatively, a needle attached to a blood bag by a length of tubing is used to collect a blood sample. A series of test tubes each having a rubber top and holding a vacuum may be sequentially punctured by a second end of the needle to collect blood samples. In some systems the blood tube may already have a bar code label attached in which case the tube in the present invention will have the label read by a bar code reader simultaneous to the biometric scan of the specimen donor. Other common means of phlebotomy or blood sample procurement are via indwelling lines such as catheters or by blood lancet puncture of skin, e.g., an infant's heel, and subsequent daubing of blood from the skin surface into capillary tubes or on to an absorbent paper card.

The supply and delivery of compatible organs for transplantation involves time critical matching of histocompatibility characteristics of the organ donor and the organ recipient. Rapid and effective tissue typing is key to supplying kidneys, hearts, lungs etc., which may only be viable for a period of hours. While the histocompatibility

parameters of the organ recipient are determined ahead of time, those of the organ donor will most probably be determined immediately after the donor is determined to have been deceased. Following the determination of death or brain death, and the determination of histocompatibility parameters, the organs may be harvested and then transported to a location where the prospective recipient has been prepared for transplantation. Under these circumstances, it is extremely difficult to carry out all of the required procedural steps in the time frame during which the harvested organ is viable.

Further, in testing of human specimens in the laboratory, there is a need from time to time for anonymity in certain circumstances, such as in double blind studies or where the donor wishes to have anonymity, as in HIV testing or autologous blood banking of HIV positive blood. In such circumstances, one known method for accomplishing the task of secure and specific identification of the specimen to the donor while maintaining anonymity has been to attach a unique alphanumeric identifying number or code via a label that is attached to the sample collection container or device.

A first limitation of such a numerical system is that one subject may give the corresponding chit to a second individual and then the second individual may portray the test material and test results as originating from and linked to him- or her-self, rather than from the true donor. A further limitation is that the alphanumeric code, if provided to the donor or researcher in the form of a disposable paper chit, may be lost. Correlation of the test specimen and container or device may then be hindered or completely corrupted. Additionally, computerized linkage of an alphanumeric code to other data may be subject to input error by a keyboard operator.

Human disease status is highly confidential information subject to potential for misuse by any of a variety of agencies or individuals. For example, some doctors will advise patients not to seek human immunodeficiency virus (HIV) testing via the doctor because the records generated in the process of testing for HIV may be used by insurance companies to deny insurance coverage to the individual requesting the test results. Some fear governmental oversight.

The reasoning seems to be that if the individual sought to ascertain HIV status information, the individual must have reason to suspect a positive HIV status. The individual therefore is adjudged likely to (i) have engaged in high-risk behavior, (ii) continue to engage in high-risk behavior and (iii) have an enhanced probability (compared to other population segments) of developing (a) HIV-positive status followed by (b) acquired immune deficiency syndrome (AIDS), presently a frequently fatal

condition. People may well be denied employment if it is suspected that they are at risk of developing an HIV-positive status or of contracting AIDS subsequent to infection by HIV.

Accordingly, it is desirable, particularly with respect to HIV testing of donated blood samples, to be tested in a way that completely protects the individual identity of the donor. One such system is provided in some states through Planned Parenthood, which collects (i) a blood sample from the donor and (ii) whatever identifying indicia the donor cares to provide, such as a pseudonym. The agency typically then (iii) links the identifying indicia, the test sample and a unique identifying code or serial number in a computer database or other log and (iv) informs the donor that test results are to be expected to be available following a set interval of one to two weeks. The one to two week interval is for shipping the test sample to a suitable laboratory or other testing facility and for receiving the results of the analysis therefrom.

The test sample and code or serial number are then (v) sent to a remote site for testing and analysis. Results are then (vi) sent back to the test site (or any other designated place). The donor (vii) returns to the test site or goes to a designated office and (viii) is advised of the test results. If warranted, (ix) appropriate counseling is provided along with follow-up services. Additionally, (x) a paper record is often provided with an indication of the test results.

Unfortunately, because the donor often provides a pseudonym, a third party has no way of knowing that a particular record is actually the product of a test conducted on samples provided by the individual presenting such a record. Moreover, the paper record is easily forged or mutilated to alter the information contained thereon, in part because there is no standard or unforgeable format for such records. This system affords an individual donor great confidence in both the anonymity and the trustworthiness of the test result, but this system does not provide the donor with any verifiable way of providing credible test results to a third party. Additionally, recent multiple-drug therapies can reduce presence of HIV and indicia of HIV to immeasurably low levels. These therapies introduce detectable levels of drugs into the bloodstream of the donor but these drugs are not tested for. Accordingly, an HIV positive person could obtain an HIV negative test result.

Accordingly, it is desirable to provide reliable data on irtfcctious status of a blood unit in an anonymous fashion whereby the person viewing the data has some assurance that the data correspond to the presenting individual. However, this alone is not necessarily sufficient because identification cards and the like may not correspond

to the bearer thereof. Therefore, it is appropriate and useful to base the correlation process on parameters unique to the individual whilst continuing to ensure anonymity of the donor, the test results and the fact that the donor had the testing performed.

There is therefore a need for some form of correlation that is unique to the individual, that is not based on a photograph of the individual or the like and that does not employ a transferable or forgeable identity device (such as an identity card). The form of correlation needs to be highly reliable and also must provide "go/no-go" identification in a short period of time (e.g., a minute or less).

Disclosure of the Invention

In one aspect, the present invention includes a biometric identification system. The identification system includes a first biometric scanner, a second biometric scanner, a processor coupled to the first and second biometric scanners and a read-write memory coupled to the processor. The read-write memory stores records, including biometric data. The system determines when two separate forms of biometric identifiers taken from an individual agree with previously-stored biometric data and thus links the individual to data that are associated with the previously-stored biometric indicia.

In another aspect, the present invention includes a system for sorting units by type. The system includes a biometric scanner and a processor coupled to the biometric scanner. The processor accepts biometric data from the biometric scanner and links the biometric data to other data to form a first record. The system also includes a read-write memory coupled to the processor. The read-write memory stores the first record in response to commands from the processor. A label reading device is coupled to the processor. The label reading device reads a second record from label on a unit in response to commands from the processor. The system further includes an output device coupled to the processor. The output device provides a "GO" signal when data corresponding to biometric data from the first record agree with data corresponding to biometric data from the second record and provides a "NO GO" signal when data corresponding to biometric data from the first record do not agree with data corresponding to biometric data from the second record. As a result, the system is able to match stored data to an individual based solely on biometric indicia.

Brief Description of the Drawings

Figure 1 is a schematic illustration of a collecting station for (i) collecting a blood sample from a donor and (ii) obtaining correlating data pertinent to the donor, in accordance with embodiments of the present invention.

Figure 2 is a schematic illustration of a collecting station for contemporaneously (i) collecting a blood sample from a donor and (ii) obtaining correlating data pertinent to the donor, in accordance with embodiments of the present invention.

Figure 3A is a schematic illustration of a blood sample analysis laboratory and computer data entry station, in accordance with embodiments of the present invention.

Figure 3B is a block diagram showing a data format for the records stored in the computer/database of Figure 3A, in accordance with embodiments of the present invention.

Figure 4 illustrates an example of use of biometric identification in drawing blood for blood typing, in accordance with embodiments of the present invention.

Figure 5 illustrates an example of use of biometric identification in blood typing, in accordance with embodiments of the present invention.

Figure 6 is a schematic illustration of a data retrieval station, in accordance with embodiments of the present invention.

Figure 7 is a flowchart describing steps involved in (i) collecting a blood sample from a donor and (ii) simultaneously collecting correlating data pertinent to the donor, in accordance with embodiments of the present invention.

Figure 8 is a flowchart describing steps involved in blood sample analysis laboratory and computer data entry in the blood sample analysis laboratory and computer data entry station of Figure 3, in accordance with embodiments of the present invention.

Figure 9 is a flowchart describing steps involved in a secure data retrieval process, in accordance with embodiments of the present invention.

Figure 10 is simplified block diagram of a system including multiple blood donation centers each equipped with the data retrieval station of Figure 6 coupled to the computer and database of Figure 3, in accordance with embodiments of the present invention.

Figure 11 is a simplified block diagram of multiple donation centers coupled to a database, in accordance with embodiments of the present invention.

Best Modes for Carrying Out the Invention and Disclosure of Invention

Figures 1 and 2 illustrate a data collection station 11 for (i) collecting a blood sample from a voluntary donor and (ii) obtaining correlating biometric data pertinent to the donor, in accordance with embodiments of the present invention. As used herein, the term "biometric data" is defined to mean a set of identifying data derived from analysis of (a) the human body anatomy of an individual, or (b) the human body function of an individual, which data is reproducible and useful for substantially uniquely

correlating to the identity of the individual from whom the data were derived. Examples from human anatomy are iris scan, fingerprint, hand geometry and facial recognition. Examples from human body function arc signature recognition and voice recognition.

The data collection station 11 includes a sample collection device or station 12 for collecting, in response to commands from a computer 13, a sample 14 for medical testing and biometric data from a biometric identification device 18. In one embodiment of the data collection station 11, the collection device 12 is a blood sample collection station. Blood specimen collection devices are available from a variety of sources including the Vacutainer line of collection devices available from Becton Dickenson Company (Rutherford, New Jersey).

The arrangement of Figure 2 ·provides a single apparatus 12' for contemporaneously or simultaneously (i) collecting a blood sample 14 from a donor and (ii) obtaining biometric data pertinent to the donor, in accordance with embodiments of the present invention.

With these types of samples, it is established practice to label the sample container 14 either prior to or after sample collection. The procedure described, for example, in The American Association Of Blood Banks Technical Manual, R. Walker, Ed.-in.-Ch., 11th Ed., 1993, pp. 14-17, on p. 15, specifies that all donor phlebotomy sample containers are to be labeled with donor identification at the donor chair but immediately prior to phlebotomy.

In many hospitals, it is written policy that the opposite occur, i.e., that phlebotomy occurs during which the donor blood enters the test tube, which is only inscribed with indicia identifying the donor after sample donation. The potential for error is present in both procedures and especially in situations where several patients with similar names but differing blood characteristics are being evaluated under emergency conditions, i.e., following an automobile accident where a number of family members are all injured in a common vehicular disaster.

One procedure for blood sample collection is as follows: (i) the patient provides positive (e g, photo) identification ("ID"); (ii) a copy of the patient ID is stapled to a requisition form; (iii) the patient's name etc. is filled out on the requisition form, together with the current date; (iv) the patient reviews the form for accuracy; (v) the patient signs a release; (vi) the container label is prepared, including the patient's name, any test that is requested, the date of collection and the collector's initials; (vii) blood samples are taken and (viii) the collector initials the seal, signs the requisition, records the date and time, lists any medications currently or recently taken, notes any

abnormalities and puts the name of requesting organization (e.g., potential or present employer, doctor) on the label.

Additionally, it will be appreciated that the sample collection station 12 may be employed, if desired, for conducting additional tests. For example, tests may be carried out for antigens or antibodies associated with infectious diseases and any other infectious or communicable conditions of the donor. This may include testing for (i) those previously successfully treated but identifiable by remaining antibodies or other indicia in samples from the donor, (ii) drugs used to treat diseases and/or (iii) "recreational" drug use, especially that associated with risk of acquiring communicable diseases, for example, via sharing of hypodermic needles, as desired or required.

It will be appreciated that detectors may be included in the blood sample collection device 12 to assess finger temperature and that sensors included with the container for the blood sample 14 can be employed to verify (i) the temperature of the specimen, (ii) that the specimen is being provided while the fingerprint is being scanned, or that the delay between initiation of these two events is only one, two, three, four or five seconds or an appropriate interval and/or (iii) that the conductivity, pH or other properties of the specimen 14 are appropriate for human blood.

In any of these embodiments, the biometric scanner 18 or 18' may provide a signal, e.g., audible or visible, to the user to inform the user that the biometric scan was successful. It will be appreciated that many different types of biometric scanners 18 could conceivably be employed to realize the desired function for the biometric scanner 18. For example, human fingerprints provide unique indicia of identity, while automatic scanning of hand geometry may also be employed for attempting to identify specific individuals.

Techniques for automatically scanning fingerprints are described in U.S. Patent No. 5,465,303, "Automated Fingerprint Classification identification System And Method," issued to Levison et al. and in U.S. Patent No. 5,222,152, entitled "Portable Scanning Apparatus For Identification Verification," issued to Fishbine et al.

Other types of biometric data successfully used for positive identification or correlation of an individual include dental records, anatomical geometries, retinal patterns, iris patterns, speech recognition or gene sequences or other chemical biodata that uniquely identify a particular individual with a high degree of confidence in the accuracy of the identification.

One system that uses fingerprint indicia but that does not necessarily store fingerprint images per se is the SACMAN™ fingerprint scanning device available from

Secure Access Control Technologies, Inc., located at 4620 S. Valley View, Suite A, Las Vegas, Nevada. This system uses a unique form of vector analysis of rastered fingerprint data taken at a high resolution, e.g., one thousand dots per inch.

A suitably programmed computer is used to process the digital data resulting from the fingerprint scan. The computer program normalizes the data, orients the features and removes noise to optimize the image. The data are converted from raster form to vector line types, which are then employed to classify the fingerprint. The system maps a scanned fingerprint into a fixed coordinate system in order to preserve the same general origin for the fingerprint data. This system has advantages of (i) a high degree of confidence in recognition of the vector line scan data, (ii) tolerance to micro feature changes and/or print contamination and (iii) security/anonymity in that this system does not necessarily store fingerprint images per se. The system also lends itself to generation of index keys for large databases, allowing very fast identification of people or data. The term "database" is used to mean a computer-sortable collection of similar electronic records each containing data describing one or more of a population of things having one or more common properties where the records arc stored in a computer memory. By inputting data and then determining that the input data agree with a portion of one (or more) of the records, the information from the remainder of the agreeing record may be linked to the source of the data. When the data disagree with all of the stored records, the source of the data may not be linked to information in any of the stored records.

Biometric identification systems that are based on scans of irises in the human eye are described in U.S. Patent No. 5,291,560, entitled "Biometric Personal Identification System Based on iris Analysis," issued to Daugman and in U.S. Patent No. 4,641,349, entitled "Iris Recognition System," issued to Flom et al. Iris scanning systems provide certain advantages in biometric identification of individuals. The iris scan does not normally change, for example, as the individual ages or is altered by a disease process. Iris scanning does not require contact with the person or conscious action by the person. Iris scanning is able to determine that the eye is that of a living human by monitoring hippus oscillations in pupil diameter which occur once or twice per second, even under uniform lighting. Accordingly, a photograph of an iris, or a contact lens imprinted with an iris image, will not exhibit the hippus oscillations characteristic of a living human being. Modern data processing techniques permit the iris of the eye to be used as an optical fingerprint having a highly detailed pattern that is unique for each individual and that is stable over many years, independent of the

degree of dilation or contraction of the pupil of the eye. The IrisIdent™ system that is marketed by Sensar Corporation of Moorestown, New Jersey is an example of a commercially available iris scanning identification system. This system is able to acquire an image of the iris when the eyelid is open from a distance of up to 36 inches using an ordinary video camera, and does not require any additional user participation. As described in U.S. Patent No. 5,291,560, an extremely high degree of confidence may be had in an identification that is obtained through iris scanning.

Feature recognition based on face geometry is described in U.S. Patent No. 4,975,969, entitled "Method And Apparatus For Uniquely Identifying Individuals By Particular Physical Characteristics And Security System Utilizing Same," issued to Tal and in U.S. Patent No. 5,012,522, entitled "Autonomous Face Recognition Machine," issued to Lambert. Identification techniques based on retinal patterns are described, for example, in U.S. Patent No. 5,369,415, entitled "Direct Retinal Scan Display With Planar Imager," issued to Richard et al. and in U.S. Patent No. 5,359,669, entitled "Remote Retinal Scan Identifier," issued to Shanley et al. Identification based on speech recognition is described, for example, in U.S. Patent No. 4,961,229, entitled "Speech Recognition System Utilizing IC Cards For Storing Unique Voice Patterns," issued to Takahashi.

Identification based on gene sequences or other chemical biodata that uniquely identify a particular individual with a high degree of confidence in the accuracy of the identification is described in U.S. Patent No. 5,270,167, entitled "Methods Of identification Employing Antibody Profiles" and in U.S. Patent No. 4,880,750, entitled "Individual-Specific Antibody Identification Methods," both issued to Francoeur.

Automated scanning of hand geometry is another form of biometric classification suitable for use with the present invention. Hand geometry scanners are described in, for example, U.S. Patent No. 5,483,601, entitled "Apparatus And Method For Biometric Identification Using Silhouette And Displacement images Of A Portion Of A Person's Hand" and in U.S. Patent No. 5,335,288, entitled "Apparatus And Method For Biometric identification," both issued to Faulkner; U.S. Patent No. 5,073,950, entitled "Finger Profile Identification System," issued to Colbert et al.; U.S. Patent No. 5,073,949, entitled "Personal Verification Apparatus," issued to Takeda et al.; and U.S. Patent No. 3,648,240, entitled "Personnel Identification Apparatus," issued to Jacoby et al.

An algorithm suitable for searching a database of entries for a match for any of the above-noted biometric classification techniques is described in U.S. Patent

No. 5,479,523, entitled "Constructing Classification Weights Matrices For Pattern Recognition Systems Using Reduced Element Feature Subsets," issued to Gaborski et al.

It will be appreciated that positive correlation of biometric data need not necessarily provide unique identification of a particular individual when a second technique for associating a specific donor with a specific test result is employed. For example, when a unique serial number known to the donor is coupled with biometric indicia for providing positive correlation of the donor and sample, the degree of confidence a third party might have that the test results correspond to the individual could be quite high (even approaching certainty) even if the biometric data alone would only provide, for example, a positive correlation carrying at least 95% confidence that the subject was correctly identified (as used herein, the term "positive correlation" means "a high order of probability of identification", i.e., a 95% certainty or better of identification). This means that the biometric data need not be exhaustive and that reduced datasets may be employed for the purpose of reducing the amount of biometric data that must be collected, transmitted and correlated.

Similarly, when two different types of biometric indicia are used to correlate a blood unit to an intended recipient or to identify an individual or to correlate the individual to a record, the odds against a false rejection or a false acceptance become remarkably small. For example, a fingerprint scan coupled with an iris scan provides a high degree of confidence in identification of the individual. As a result, the resolution of the biometric data that are collected and processed need not be as high as would be required in a system that only employed one type of biometric indicator. This allows the correlation of the biometric data to be carried out with fewer data elements and thus to be more rapid.

In another embodiment, one of the biometric identification steps may be carried out through an electronic scanner while another biometric identification step is carried out by a human operator. For example, an iris scan might be carried out by an electronic scanner and the result processed in a computer while a human compares a previously-stored image of a biometric indicator to an image of the same kind of biometric indicator just taken from the presenting individual. Examples of images that lend themselves to comparison by humans include facial photographs and fingerprint images. When the human operator is satisfied that the two sets of biometric data do or do not match, the human operator may input data to the computer to indicate the decision that the human operator has made regarding the comparison.

The sample collection station 11 yields the sample 14 and the sample 14 is then (preferably simultaneously) labeled by a labeling device 20. The sample collection station 11 includes an input such as a keyboard 22, whereby additional data may be entered by medical personnel for inclusion on the label of the sample 14 and/or included with biometric correlation data from the biometric correlation device 18. The test date may also be included on the label of the sample 14. Alternatively, the sample container tube may have a bar code already in place which is read by a bar code reader simultaneous to the sample donor biometric scan.

The labeling device 20 may be a conventional laser printer, bar code printer or other printing or labeling device. Biometric correlation data from the biometric correlation device 18, a serial number or other correlating indicia, the date of the test and any other desired data are then linked together and may be supplied via an external link 23 for shipment to a database (not shown in Figures 1 or 2). The labeled sample 14 may then transported to a laboratory for analysis.

It will be appreciated that other types of recording media may be usefully employed for storage of the biometric information. For example, an integrated circuit or chip (not shown in Figures I or 2) may be built into the wall of the container 14 that holds the sample, which integrated circuit is coupled to a small antenna (not shown) built into or mounted on the wall of the container 14. The antenna may allow power to be electromagnetically coupled to the chip when it is in the vicinity of another antenna (e.g., built into or mounted on the needle or needle holder) that is supplying the electrical power. These antennae may also permit data to be written to the chip and read from the chip, much as data are read in electronic toll collection devices deployed around the nation (e.g., the IPASS system used in the Chicago area). Alternatively, a physical electrical interconnection could be employed, much as data arc read from and written to "smart cards" used for financial transactions.

In one embodiment of the present invention, the electronic link 23 is an encrypted digital link and may be effected via telephone line, for example. In one embodiment of the present invention, the computer 13 supplies the serial number to a printer (not illustrated), which prints out a slip bearing the optional serial number for later use by the donor.

The labeled sample 14 is transferred via a link 24 to a sample analysis station (not shown in Figures 1 and 2). Transfer via the link 24 may be by common carrier to a remote site (e.g., a central testing facility) or to another room in the same facility. This could be effected via the Confide HIV Testing Service™ provided via Direct

Access Diagnostics, a subsidiary of Johnson and Johnson, Inc. Direct Access Diagnostics has obtained FDA approval for an over-the-counter blood sample collection kit and testing procedure similar to the testing approach used by Planned Parenthood, i.e., providing the tested individual with great confidence in the accuracy of the test results but not providing a third party with any assurance that the test result corresponds to the presenting individual.

The system of Figure 2, wherein the biometric scanner 18 is integrally combined with the sample collection device 12 to provide a combined scanner/sample collection device 12', is an arrangement for the practice of the present invention. By collecting the sample 14 contemporaneously or simultaneously with assessment of biometric indicia, assurance that the sample 14 and the labeling biometric indicia correspond to one and the same person is provided without requiring the presence of a human monitor in order to ensure compliance. For example, a small blood sample 14 may be taken from the tip of one finger (e.g., the middle finger) during the scanning of biometric data from the donor's hand or at least during a single insertion of the donor's hand into the combined scanner/sample collection device 12'.

This arrangement avoids a situation that could occur if the donor were allowed to simply volunteer a previously-collected sample 14 when having biometric data collected. In the latter scenario, there is no assurance that the sample 14 actually came from the donor, rather than the donor's friend, child or pet. Apparatus for collection of small blood samples 14 are conventional in the medical industry where such procedures have been employed for decades for testing for, e.g., phenylketonuria in newborns. Semi-automatic blood sample collection apparatus are also conventional.

A first advantage of taking the test sample 14 either under supervision of a neutral medical person or in conjunction with the collection of correlating biometric data is that this assurance can be provided to third parties. An additional advantage is realized in that the donor need not reveal a personal address or telephone number to an agency, such as Direct Access Diagnostics, where this information might be discoverable by others. A further advantage accrues if the donor can only activate access to the test results by first reviewing the test result with a trained counselor or medical doctor. In-person, face-to-face counseling with appropriate compassion, concern and medical interpretation is then available to the donor in the unfortunate event of a positive test result for HIV or other curable or incurable conditions.

Figure 3A is a schematic illustration of a blood sample analysis laboratory and computer data entry/storage station 25, in accordance with an embodiment of the present

invention. Incoming samples 14 arrive via the link 24 and are identified by a label reader 26 to determine the serial number or other correlating indicia associated with the biometric data and to be associated with results of analysis of the sample 14. The sample 14 is supplied to a sample analyzer 27 via the link 24 and an analysis of the contents of the sample 14 is performed and communicated to a computer/database 29. The results of the analysis of the sample 14 are coupled to the biometric correlation data, and, if desired, to the optional serial number by the computer and database 29.

Figure 3B is a block diagram showing a data format for a computer record 36 stored in the computer/database 29 of Figure 3A, in accordance with embodiments of the present invention. With most forms of biometric identification, the amount of data 37 required in order to represent the biometric information is known, while the amount of data 38 appended to the biometric data may vary from one record 36 to another or over time within one record 36. For example, U.S. Patent No. 5,291,560 discusses generation of iris codes 37 having a length of 2,048 bits or 256 bytes from an iris image of 262,000 bytes (corresponding to a 512 x 512 pixel imaging device with a per-pixel resolution of one byte). The amount of biometric data that can be included in each biometric data field 37 corresponds to limits to performance of the system in identifying individuals or detecting impostors.

In contrast, when a patient's entire medical history is a portion of the medical data field 38 appended to the biometric data field 37, the medical data field 38 may be quite large and may include various kinds of graphical data, e.g., X-ray, magnetic resonance imaging or positron emission tomography data or the like. In some embodiments, the biometric data field 37 may be subdivided into several sections to accommodate, e.g., multiple fingerprints from several of one patient's fingers, multiple fingerprints from multiple people, e.g., the patient and the doctor, or a newborn and the mother, or to accommodate multiple kinds of biometric data, e.g., fingerprint data and iris data, taken from one patient or from multiple individuals. For example, collecting biometric data from both the mother and the newborn, linking these data into a single record 36 and then using that record 36 as a basis for comparison when the mother and the newborn leave the hospital can prevent the problem of a baby from a different mother being sent home with the mother that is leaving the hospital. For example, the mother's biometric data might be taken at checkout. These data, and the data taken in conjunction with the birth, may be fingerprint, iris or other biometric data. The mother's data can then be compared by the computer 29 of Figure 3A to records 36 (Figure 3B) stored in the database 29. When a match is found, biometric data, such as fingerprint

data, from the newborn the hospital gives to the mother to take home can be compared to the biometric data stored with the mother's biometric data to determine if this is the correct newborn.

In some embodiments, a portion of the record 36 may be reserved for indicating the total size of the record 36. When an existing record 36 is found to match biometric data input as a part of storing new medical data from analysis of a new sample 14, for example, the new medical data may be appended as a new portion 38' of the medical record 36. This allows a medical history to be built up in the record 36 in a fashion that is consistent with the longitudinal view typical of Western medical practice.

Figure 4 illustrates an example of use of biometric identification in drawing blood for blood typing, in accordance with embodiments of the present invention. Following collection of biometric indicia, a series of labels 40 are printed bearing data 41 having a correspondence to biometric indicia of the patient. In the examples of Figures 4 and 5, finger print data are literally reproduced on the labels 40, however, it will be appreciated that other types of biometric indicia 41 could be used and that these might be in machine-readable only form, e.g., binary data stored in a memory device that may be a nonvolatile memory integrated circuit and that forms a portion of the label 40 or blood sample container 42. Additionally, the labels 40 may optionally include a bar code 41' and/or a patient's name 41".

In one embodiment, in a first step, a first of the series of labels 40 bearing biometric indicia 41 is attached to the blood sample container 42 containing the sample 14 (Figures 1 and 2) of blood from an intended transfusion recipient. In one embodiment, the biometric data are gathered from the patient and written to the label 40 as the blood sample 14 is drawn. In a second step, a second of the series of labels 40 is placed on, or data corresponding to biometric indicia 41 are written to, a wrist band 43 on that patient's wrist. In one embodiment, the data are recorded on or in the wrist band 43 as the blood sample 14 is drawn.

Figure 5 illustrates an example of use of biometric identification in blood typing, in accordance with embodiments of the present invention. In one embodiment, third through twelfth labels 40a-40j of the series of labels 40 are placed, one each on a series of blood sample containers 42a-42j, respectively. The blood sample containers 42a-42j are used during the crossmatch procedure as follows: 42a - Anti-A; 42b - Anti-B; 42c - Anti-D; 42d - Screen 1; 42e Screen 2; 42f - Screen 3; 42g - D control; 42h - Reverse A; 42i - Reverse B; 42j cell suspension tube containing washed red blood cells from the intended transfusion recipient, according to the procedure specified in the American

Association of Blood Banks procedure manual. Once blood aliquots from the donated units selected for crossmatch testing are tested in the standard manner and a unit 42k is found to be crossmatch compatible for the prospective recipient, the unit 42k is labeled with the label 40k representing the finding of the medical technologist that the unit 42k is compatible with the blood sample in the blood sample container 42. The unit 42k then can be linked to the patient or the patient's chart through comparison of labels 40 bearing the same biometric indicia or to the patient into whom the transfusion is to be given through re-taking of the biometric data.

When blood testing is performed for tissue typing in anticipation of transplantation, HLA (human leukocyte antigen) testing is performed. A match of donor and intended recipient HLA data indicates a substantially reduced probability of rejection of the transplanted organ.

In one embodiment, a nurse requesting blood will attach one of the series of labels 40 directly to a transfusion request form for that patient. When a nurse or orderly visits the blood bank to pick up the unit 42k identified as being crossmatch compatible, the nurse or orderly compares the data on the label 40 on the transfusion requisition to the data on the label 40 on the unit 42k to verify that the biometric indicia or data corresponding thereto are identical for the two labels 40 and 40k. The comparison may be visual or may be electronic or both.

In one embodiment, prior to administering blood from the unit 42k, the nurse uses a bar code reader (not illustrated) to read the bar code 41' on the label 40k. The computer/database 29 of Figure 3 receives the bar code 41' and uses this to access the stored record 36 of the biometric data 37 corresponding to the patient. The patient then provides new biometric data, which are transmitted to the computer/database 29. The computer/database 29 then compares the stored biometric data 37 to the new biometric data and/or to the biometric data stored on the label 40k. The data 38 added to the database data 36 includes the number of the unit(s) found crossmatch compatible for that patient. In one embodiment, the biometric data recorded on the label 40k are compared to the new biometric data. When the biometric data are identical, the nurse administers the transfusion. When the biometric data do not match, the nurse does not administer the transfusion and may request a re-draw of a blood sample 14 from the patient and have this re-tested for crossmatch to identify another unit 42k. As a result, transfusion reaction in the patient is avoided.

When the biometric indicia on the label 40k comprise a rendition of a fingerprint, visual inspection of a finger print image taken from the patient and comparison to the

rendition on the label 40k may be substituted for the electronic comparison by the computer/database 29.

In one embodiment, a fluid-dispensing unit includes a tube 44 joining the fluid reservoir forming the unit 42k and a needle (not illustrated) used to administer the transfusion. The needle or the tube 44 includes a valve 45, which may be an electrically-operated valve, controlled by the computer/database 29, which provides "GO"/"NO GO" signals. In this embodiment, the valve 45 acts as a lock and does not open when the biometric data on the label 40k and the new biometric data do not match. The valve 45 opens when the biometric data on the label 40k and the new biometric data, be., that biometric data derived from a biometric scan taken from the intended recipient at the bedside by the nurse just prior to transfusion of blood from the unit 42k, do match. As a result, blood can only flow from the unit 42k to the patient when the biometric data match. The valve 45 may be coupled electronically to the computer/database 29 by a wired link or by a conventional radio frequency, ultrasonic or optical link.

When the transfusion is one involving cord blood, the unit 42k will have been labeled with biometric data taken from the newborn at or near the time of birth. These biometric data may correspond to the newborn's irises, fingerprints, palmprints, toeprints or footprints. In this way, a biometric indicator known to vary in response to aging only in size from birth onward provides positive correlation that the unit 42k of cord blood corresponds to this particular infant. A secondary data field may include the birth mother's fingerprint or other biometric data.

Figure 6 is a schematic illustration of an embodiment of a data retrieval station 46 of the present invention. The data retrieval station 46 includes the biometric identification device 18 coupled to the database 29 of the computer data entry station 25 (Figure 3) via the link 23. The data retrieval station 46 also includes a display 47 and optionally includes a data entry device 48, both also linked to the database 29 via the link 23. The data entry device 48 includes a keyboard in one embodiment of the present invention. When results from medical testing are linked to a database via a biodata key, i.e., a set of biometric data from the specimen donor, it becomes possible for the results to be registered or escrowed with a third party organization whereby another hospital or other entity may access them, e.g., view them on the display 47, using the data retrieval station 46.

Figure 7 is a flowchart describing steps involved in a process 50 for (i) collecting the blood sample 14 (Figures 1 and 2) from a donor and (ii) obtaining

correlating data pertinent to the donor, in accordance with embodiments of the present invention. The process 50 begins in a step 53 with taking of a biometric correlation reading that is digitized for further processing by the computer/database 29 (Figure 3) and that optionally is also linked to the date when the biometric data were taken. In the step 53, a blood sample 14 is also collected, optionally under the supervision of one or more witnesses to both sample collection, and the taking of the biometric correlation reading, in order to ensure the integrity of the data collection and correlation processes.

Alternatively, the step 53 of sample collection may be automated by, for example, combining a biometric scan with a blood sample collection device such that the sample 14 could only have come from the individual donor from whom biometric correlation data were collected. When blood samples 14 are collected, additional confirmation of the integrity of the testing and correlation processes may be effected by determining the temperature of the collected blood sample 14 (e.g., via a thermocouple, thermistor or liquid crystal thermometer) and/or by monitoring electrical conductivity or other properties of the sample 14.

Similarly, a fingerstick blood sample collected simultaneously with a finger print biometric scan by drawing the sample 14 from the finger from which the fingerprint is being taken and at the same time as the fingerprint is scanned provides similar assurances. These methods have the advantage of allowing the sample collection station 12' (Figure 2) to operate without requiring human operators while still protecting the integrity of the system, i.e., a third party could still reasonably have great confidence that the medical information derived from the sample 14 corresponds to the individual providing matching biometric data.

In a step 56, a numeric correlation number or serial number is optionally assigned by the computer 13 within the station 11 (Figures 1, 2) or by the computer/database 29 of the computer data entry station 25 (Figure 3). In a step 58, the serial number, biometric data, test date and sample 14 are linked to form a record 36 (Figure 3A) by (i) printing a correlating label on the sample 14 container via the labeling device 20 (Figures 1, 2) and (ii) transmitting the test date, biometric data and optional serial number via the link 23 to the computer/database 29 (Figure 3). In a step 59, the serial number is optionally made available to the donor via a slip from a printer (not shown). In a step 60, the labeled sample 14 is transported via the link 24 (Figures 1, 2) to the blood sample analysis laboratory and computer data entry station 25 (Figure 3). The data collection process 50 then ends.

Figure 8 is a flowchart describing steps involved a process 70 for blood sample 14 (Figures 1 and 2) analysis and computer data entry in the blood sample analysis laboratory and computer data entry station 25 (Figure 3), in accordance with embodiments of the present invention. It will be understood by those of skill in the art that while the process 70 discusses blood samples 14, any medical data may be stored in accordance with the disclosed technique. The process 70 begins when incoming samples 14 are transported via the link 24 to the label reader 26 (Figure 3). In a step 72, the biodata, i.e., the biometric scan data from the specimen donor, test date and/or optional serial number on the label 40 (Figures 4 and 5) of the sample 14 are read by the label reader 26 (Figure 3). In a step 74, the sample 14 is analyzed to determine infectious status, presence of antigens or antibodies associated with past or present infectious disease of the donor and/or presence of therapeutic or "recreational" drugs or metabolites thereof. In a step 76, the results of the analysis, optionally including the date when the analysis was performed and also optionally including data describing the test parameters and/or testing institution, are linked to the sample collection date, biometric correlation data and or serial number.

A query task 78 then interrogates the database 29 using information corresponding to the biometric data from the label 40 (Figures 4 and 5) on the sample 14 to determine if the biometric data from the label 40 match any records 36 (Figure 3A) in the database 29. When the query task 78 determines that no records 36 match the biometric data from the label 40 of the sample 14, a new record 36 (Figure 3A) is formed, comprising a biometric data portion 37 and a medical data portion 38, and the new record 36 is used to created a new entry in the database 29 (Figure 3) in a step 80. The analysis process 70 then ends.

When the query task 78 determines that a record 36 does match the biometric data from the label 40 on the test sample 14, either the medical data portion 38 of the record 36 is overwritten with the new test results, or a new medical data portion 38' of the record 36 is created, including the added medical data. The new medical data portion 38' is appended to the existing record 36, in a step 82. The analysis process 70 then ends.

It is desirable to be able append additional medical data 38' to existing medical records 36 (Figure 3A) for many reasons. For example, in situations where a patient is receiving transfusions of blood for more than a few days, the blood typing and crossmatch compatibility information is updated every forty-eight hours. A fresh blood sample 14 is drawn and is tested as described above in association with Figure 5. This

is done to avoid a situation where the patient has developed a new antibody during the last 48 hours that could influence crossmatch compatibility. Accordingly, when the patient has developed an additional antibody, updating the record 36 by appending additional medical data 38' relevant to this is useful.

It will be appreciated that stored data 36 may have come from another source, i.e., from a testing system outside of the system described thus far. In these instances, when it is determined that the data 38 provide an acceptable degree of integrity, these may be linked to the biometric data 37 from the donor, optionally along with data describing the provenance of the test data (including test dates, sample collection dates and the like). The resultant composite record 36 is stored in the computer/database 29 of Figure 3 in a fashion analogous to that used for data 38 derived from test samples 14 taken as indicated hereinabove.

An incidental benefit that accrues with regard to billing for lab testing and the like, especially when carried out by third party billing agencies, is a viable means to link billing records to testing charges and to the correct billable party. Often, especially within an extended family, charges are billed out inappropriately, for example, to one family member for services provided to a different family member. Similarly, when getting medical records, a resemblance of names often results in confusion when a chart for, e.g., the patient's father is pulled, despite dissimilarities in age, social security number, clinic ID number and the like. These transactions tend to be time consuming, frustrating and unnecessarily expensive. By linking the patient's biometric data to the test sample 14, the test results and thereby to the bill, human error in preparing the bills for medical services can be avoided, the correct party obtains and pays the bill and the bill can be processed more readily by insurance carriers. A biometric data terminal similar to that at the blood bank would be placed at the billing office. Those who wish to verify their bill can visit and by input of their biometric can call up the file of tests and the associated charges for which they are responsible to pay.

Figure 9 is a flowchart describing steps involved in a secure data retrieval process 90, in accordance with embodiments of the present invention. The data retrieval process 90 begins when a person, who may be, for example, a prospective blood donor, approaches the data retrieval station 46 (Figure 6). In a step 92, the biometric data collection device 18 is accessed. The biometric data collection process may be initiated by proximity to the biometric data collection device 18, may be initiated by the person who approached the biometric data collection device 18 or may be initiated by medical staff. In a step 94, the biometric data collected in the step 92 are transmitted to the

computer/database 29 of Figure 3 via the link 23. A query task 96 then determines if the biometric data transmitted in the step 94 match any of the records 36 (Figure 3A) that are stored in the computer/database 29.

In a step 98, the display 47 (Figure 6) provides an indication that no match was found when the query task 96 determines that no records 36 match the transmitted biometric data. The process 90 then ends.

In a step 100, in one embodiment, the computer and database 29 transmits a signal indicative of a match when the query task 96 determines that the input biometric data match corresponding biometric data 37 in the database 29. The computer 29 responds by transmitting a signal indicating that the medical data 38 are part of the computer record 36 that included the biometric data 37 that matched the transmitted biometric data. The transmitted signal may be used to provide, for example, a "GO/NO-GO" signal for a transfusion, for example, or may include the stored medical data 38. If the stored medical data 38 include a great deal of information, it may be organized or searchable by date, topic and the like in order to facilitate inspection. In a step 101, the data are displayed on the display 47 for a predetermined interval. In a step 102, the display 47 is erased. The process 90 then ends.

The process 90 does not require identification of any kind beyond biometric data, but is compatible with other types of medical record storage that depend on a patient serial number or patient name in order to access records. Processes that rely only on these methods, and processes that combine biometric data with other information to locate records, are compatible with the system needed in order to access data using the process 90.

It will also be appreciated that in some settings, a doctor may wish to be able to store medical information in such a fashion that it can only be recalled by the patient. For example, with genetic testing for various disorders and abnormalities, there may be concern that these data, if made available or if seized from the doctor, could be used to discriminate against the individual. Some fear that if the genetic test results were known to industry, discrimination may occur against individuals with genetic predisposition to disease. Governmental and private concern for implications of a positive genetic test result, as for example for BRCA-1, are well known.

The need for individuals to know their own genetic predisposition and medical personnel to watch for and screen for any such disease development is key. Despite potential governmental regulations which offer protection from discrimination based on genetic predisposition, a need for allowing medical care while keeping test results private

is seen. The invention herein disclosed includes methods and systems that can accomplish this by only allowing the test results to be viewed when the patient to whom the results are pertinent provides a biometric identification.

Figure 10 is a flowchart of a process 110 for collecting more than one type of biometric data and using those biometric data to match to a specific record 36 (Figure 3A) stored in the computer/database 29 of Figure 3. The process 110 begins with a step 112 of collecting first biometric data. A query task 114 compares the first biometric data with biometric data records 37 stored in the computer/database 29. Alternatively, the query task 114 may be carried out by a human operator. For example, a fingerprint match may be made by medical personnel viewing a first image from a fingerprint scan taken at the time of the donation and a second image from a fingerprint scan taken at or near the time of the comparison. When the query task 114 indicates that the first biometric data do not match any record 36, a first signal is activated in a step 116. The process 110 then ends.

When the query task 114 determines that the first biometric data do match biometric data 37 in a record 36, second biometric data are collected in a step 118. A query task 120 then determines if the second biometric data match biometric data 37 in the same or a corresponding record 36. When the query task 120 determines that the second biometric data do not correspond to the same or a corresponding record 36, the first signal is activated in the step 116. When the query task 120 determines that the second biometric data do correspond to the same or a corresponding record 36, that record 36 may be accessed in a step 122 and a second signal indicates identification of the stored record 36 corresponding to that paticut in a step 124. In either case, the process 110 then ends.

In the query task 120, the second biometric comparison, for example based on iris scans, may be carried out, where a first iris scan was taken at the time of donation and a second iris scan was taken from the same eye as the first iris scan. The second iris scan is taken at or near the time of comparison.

Where a patient has prepared for elective surgery by autologous blood specimen donation, the surgeon will, prior to the surgery, order blood to be transfused to the patient. In one embodiment, as the blood units 42 (Figure 5) are selected from the blood bank and delivered to the operating room, dual biometric datasets are used to verify the identity of the intended recipient using the process 110 of Figure 10.

When two different types of biometric indicia are used to correlate a blood unit 42 to an intended recipient or to identify an individual or to correlate the individual to

a record, the odds against a false rejection or a false acceptance become remarkably small. For example, a fingerprint scan coupled with an iris scan provides a high degree of confidence in identification of the individual. As a result, the resolution of the biometric data that are collected and processed need not be as high as would be required in a system that only employed one type of biometric indicator. This allows the correlation of the biometric data to be carried out with fewer data elements and thus to be more rapid.

In another embodiment, one of the biometric identification steps in the query tasks 114 and 120 of Figure 10 may be carried out through an electronic scanner 18 while another biometric identification step is carried out by a human operator. For example, an iris scan might be carried out by an electronic scanner 18 and the result processed in a computer 29 while a human compares a previously-stored image of a biometric indicator to an image of the same kind of biometric indicator just taken from the presenting individual. Examples of images that lend themselves to comparison by humans include facial photographs and fingerprint images. When the human operator is satisfied that the two sets of biometric data do or do not match, the human operator may input data to the computer to indicate the decision that the human operator has made regarding the comparison.

Figure 11 is simplified block diagram of a system 130 including multiple blood donation centers 132, 132' each equipped with the data retrieval station 46 of Figure 6 coupled to the computer and database 29 of Figure 3 in accordance with embodiments of the present invention. Each of the blood donation centers 132, 132' is able to retrieve records 36 (Figure 3A) from the central computer and database 29 using the process 90 of Figure 9 by taking a biometric reading from a person for whom a record 36 exists in the database 29. This system describes a specific embodiment adapted to use, for example, data corresponding to fingerprint data (e.g., data from the SACMAN™ system) or with data corresponding to iris data (e.g., data from the IrisIdent™ system).

In an alternative embodiment, the centers 132, 132' can be other kinds of institutions likely to be visited by a substantial proportion of the population in a given geographical or geopolitical area. Examples of such institutions 132, 132' might include driver's license registration centers, voter registration centers and social security and other public benefits offices, among others. During normal business operations, biometric data may be collected using biometric identification devices analogous to biometric scanners 18 of Figures 1, 2 and 6. Epidemiological data may also be collected and entered on a data entry device 23 (Figure 6) and coupled with the

biometric data, forming a computer record 36 (Figure 3B) that is stored in the database 29 (Figure 3A). In one embodiment, this allows a national medical/epidemiological database to be collected. The computer record 36 may be augmented with other data, e.g., identification name/number, or medical/epidemiological data from other sources. The database can be sorted based on existing records of the voter such as age, past disease markers, gender, location of residence, and other available data to allow demographic survey of disease patterns over time.

The foregoing detailed description of the various embodiments of the invention have been particularly directed toward separate facilities for data storage and data retrieval. It will be appreciated that embodiments of the invention may be equally useful for systems where data storage is also performed at each data retrieval station, for example.

It will be appreciated that a system for (optionally, anonymously) testing for infectious disease and or associated antigens or antibodies and/or other therapeutic or "recreational" drugs or metabolites has been described that does not require the donor to carry any identification card or to provide any photograph or home address to the system. The system may permit twenty-four hour access to the data in a fashion that (i) provides high credibility to the user as to the accuracy of the test result and the applicability of the test result to the user and (ii) provides high credibility to another person that the test results and test sample collection date correspond to the observable user and accurately reflect the infectious/communicable status of the donor and/or presence of associated antigens or antibodies and\or other therapeutic or "recreational" drugs as of the date of sample collection, without compromise of the identity of either party.

It will be appreciated that need for a serial number or at least need for the donor to have any knowledge of a serial number could be eliminated by employing the biometric data alone as means for accessing the system. Measurement of finger temperature or observation of the scanning process by both parties each provide assurance that no facsimile of a fingerprint is being employed to "fool the system."

Various changes and modifications to the embodiment herein chosen for purposes of illustration will readily occur to those skilled in the art. For example, other types of diseases or genetic predispositions may be tested for, to effectuate a combination of capabilities as may be desired tor a specific application. To the extent that such modifications and variations do not depart from the spirit of the invention, they are

intended to be included within the scope thereof which is assessed only by a fair interpretation of the following claims.

Having fully described the invention in such clear and concise terms as to enable those skilled in the art to understand and practice the same, the invention claimed is:

CLAIMS

1. A biometric identification system comprising:

a first biometric scanner;

a second biometric scanner;

a processor coupled to the first and second biometric scanners; and

a database coupled to the processor and storing records including biometric data.

2. The biometric identification system of claim 1 wherein the first biometric scanner is a fingerprint scanner.

3. The biometric identification system of claim 2 wherein the second biometric scanner is an iris scanner.

4. The biometric identification system of claim 2 wherein the fingerprint scanner is coupled to a display, the display displaying first and second sets of dermatoglyphic data, wherein the first set of dermatoglyphic data were read from a database and the second set of dermatoglyphic data were scanned from a human being by the first biometric scanner.

5. The biometric identification system of claim 1 wherein the processor compares biometric data from the first and second biometric scanners to biometric data contained in the records in the read-write memory to locate a first record including data corresponding to biometric data in the record that correlate with the biometric data from the first and second biometric scanners.

6. The biometric identification system of claim 1 wherein the processor assembles data including data corresponding to biometric data from the first and second biometric scanners into a first record and the first record is stored in the read-write memory in response to commands from the processor.

7. A system for sorting units comprising: a read-write memory storing records including biometric data; a processor coupled to the read-write memory, the processor accepting input biometric data and comparing the records to the input biometric data to locate a first record including data correlating with the input biometric data; and a labeling device coupled to the processor, the labeling device for labeling a unit with data from the first record in response to commands from the processor.

8. The system of claim 7 wherein the unit comprises a blood unit storing blood-derived fluid.

9. The system of claim 7 wherein: the unit comprises a blood unit; and the first record comprises data corresponding to biometric data relating to a crossmatch

compatible recipient for whom the blood unit is intended to provide blood for a transfusion.

10. The system of claim 7 wherein the input biometric data comprises biometric data chosen from a group consisting of iris data and fingerprint data.

11. The system of claim 7 wherein: the unit comprises a read-write memory coupled to the unit; and the labeling device comprises a link to the read-write memory whereby the record may be transmitted through the link and stored in the read-write memory and the record may be read back from the read-write memory through the link.

12. A system for sorting units by type comprising:

a biometric scanner;

a processor coupled to the biometric scanner, the processor accepting biometric data from the biometric scanner and linking the biometric data to other data to form a first record;

a read-write memory coupled to the processor, the read-write memory storing the first record in response to commands from the processor;

a label reading device coupled to the processor, the label reading device reading a second record from a label on a unit in response to commands from the processor; and

an output device coupled to the processor, the output device providing a "GO" signal when data corresponding to biometric data from the first record correlate with data corresponding to biometric data from the second record and providing a "NO GO" signal when data corresponding to biometric data from the first record do not correlate with data corresponding to biometric data from the second record.

13. The system of claim 12 wherein the unit comprises a blood unit storing blood.

14. The system of claim 12 wherein: the unit comprises a blood unit; and the record comprises data corresponding to biometric data relating to a crossmatch compatible recipient for whom the blood unit is intended to provide blood for a transfusion.

15. The system of claim 12 wherein the biometric scanner comprises a biometric scanner chosen from a group consisting of an iris scanner and a fingerprint scanner.

16. The system of claim 12 wherein: the unit includes a read-write memory coupled to the unit and the label reading device comprises a link to the read-write memory over which the record may be read from the read-write memory.

17. A fluid dispensing system comprising:

a biometric scanner;

a bar code reader;

a processor coupled to the biometric scanner, the processor retrieving a stored biometric record in response to a bar code from the bar code reader and comparing signals from the biometric scanner to the stored biometric record; and

a fluid dispensing unit including a lock, the lock allowing fluid to be dispensed when the signals from the biometric scanner correlate with the stored biometric record and the lock not allowing fluid to be dispensed when the signals from the biometric scanner do not correlate with the stored biometric data.

18. The fluid dispensing system of claim 17 wherein the fluid dispensing unit comprises a blood unit.

19. The fluid dispensing system of claim 17 wherein the biometric scanner is chosen from a group consisting of a fingerprint scanner and an iris scanner.

20. A blood transfusion system comprising:

a fluid reservoir;

a dispensing tube coupled to the fluid reservoir;

an electrically-operated valve having two states, the valve coupled to the dispensing tube, the valve preventing dispersing of fluid in the fluid reservoir via the dispensing tube in one state and allowing dispensing of the fluid in another state;

a label coupled to the fluid reservoir, the label containing machine-readable information corresponding to biometric data; and

a link to a computer providing signals in response to the machine-readable information that determine when the electrically-operated valve is in the first or second states.

21. The blood transfusion system of claim 20 wherein the label comprises a nonvolatile memory integrated circuit.

22. A method for storing a computer record comprising:

forming a first data field having a first size, the first data field storing data derived from a biometric scan of an individual;

forming a second data field having a second size, the second data field storing data describing medical information relative to the individual;

appending the second data field to the first data field to form the computer record; and

storing the computer record in a database.

23. The method of claim 22 wherein the act of forming a first data field comprises forming a first data field storing biometric data derived from scanning an iris of the individual.

24. The method of claim 22 wherein the act of forming a first data field comprises forming a first data field storing biometric data derived from scanning a fingerprint of the individual.

25. The method of claim 22 wherein the act of forming a first data field includes:

forming a first data field having a first fixed size;

forming a first data subfield within the first data field, the first data subfield including first biometric data from the individual; and

forming a second data subfield within the first data field, the second data subfield including second biometric data from the individual.

26. The method of claim 25 wherein the act of forming a first data subfield includes forming a first data subfield storing first biometric data derived from scanning a fingerprint of the individual.

27. The method of claim 26 wherein the act of forming a second data subfield includes forming a second data subfield storing second biometric data derived from scanning an iris of the individual.

28. The method of claim 26 wherein the act of forming a second data field includes storing data describing medical billing information.

29. A method for linking at least one individual to a stored computer record comprising:

taking first biometric data;

comparing the first biometric data to a series of stored computer records;

activating a first signal when none of the stored computer records provide a match to the first biometric data;

taking second biometric data;

comparing the second biometric data to the series of stored computer records;

activating the first signal when none of the stored computer records match the second biometric data; and

activating a second signal when both the first and second biometric data match one of the stored computer records.

30. The method of claim 29 wherein the act of taking first biometric data comprises taking fingerprint data.

31. The method of claim 29 wherein the act of taking second biometric data comprises taking iris data.

32. The method of claim 29 wherein the act of comparing the second biometric data comprises comparing the second biometric data to a record that matched the first biometric data.

33. A method for linking an individual to a stored computer record comprising:

taking first biometric data;

comparing the first biometric data to a stored computer record;

activating a first signal when the stored computer record disagrees with the first biometric data;

taking second biometric data;

comparing the second biometric data to the stored computer record;

activating the first signal when the stored computer record does not match the second biometric data; and

activating a second signal when both the first and second biometric data match the stored computer record.

34. The method of claim 33 wherein the act of comparing the first biometric data to a stored computer record comprises comparing the first biometric data to a stored computer record retrieved using a match to a bar code.

35. The method of claim 33 wherein the act of comparing the first biometric data to a stored computer record comprises comparing the first biometric data to a stored computer record retrieved from a memory.

36. The method of claim 33 wherein the act of comparing the second biometric data to a stored computer record comprises comparing, by a computer, digital information corresponding to the second biometric data to digital information stored in a memory.

37. A method for blood transfusion comprising: reading biometric data from a patient; comparing the biometric data to stored records; and allowing blood to be transfused into the patient when the stored records and the biometric data correlate.

38. The method of claim 37 wherein the act of allowing blood to be transfused into the patient comprises allowing blood that was previously donated by the patient to be transfused into the patient when the stored information and the biometric data correlate.

39. The method of claim 37, further comprising obstructing transfusion of the blood when the stored data and the biometric data do not correlate.

40. A method of matching potential organ donors and recipients comprising:

collecting histocompatibility and biometric data from a first population of potential organ donors into computer records in a first database;

identifying a potential organ donor;

taking a biometric reading from the potential organ donor;

comparing the biometric reading to the biometric data to determine if the potential organ donor is one of the first population;

locating a computer record having information regarding the one of the first population in the first database via matching of the biometric reading to biometric data in one of the computer records;

extracting stored histocompatibility data corresponding to the matching biometric data from the one of the computer records; and

matching stored histocompatibility data from the one of the first population to a computer record of histocompatibility data for potential recipients in a second database to identify a crossmatch compatible recipient in need of an organ transplant.

41. The method of claim 40 wherein matching stored histocompatibility data comprises:

matching the biometric reading with a record from the first database, the record including first histocompatibility data; and

comparing the first histocompatibility data to records from the second database that include histocompatibility data for a second population of persons in need of an organ transplant to identify those of the second population that are histocompatible with the potential organ donor.

42. A method for storing and accessing medical data comprising:

collecting first biometric data from an individual;

determining whether a donor status of the individual is that the individual is suitable as a blood donor or is that the individual should be deferred;

creating a computer record comprising the first biometric data and data describing donor status; and

storing the computer record in a database.

43. The method of claim 42, further comprising:

collecting second biometric data from a presenting individual;

searching the database using the second biometric data as a biodata key to locate any computer record including biometric data matching the second biometric data; and

retrieving donor status data from any record having biometric data matching the second biometric data.

44. The method of claim 43, further comprising:

collecting second biometric data from a presenting individual in a second donor center;

searching the database using the second biometric data as a biodata key to locate any computer record including biometric data matching the second biometric data; and

retrieving the donor status data from any record having biometric data matching the second biometric data.

45. A method for dispensing blood comprising:

obtaining a unit of blood that is compatibility cross-matched to a patient, the unit of blood including information storage capacity having data stored therein;

collecting the data from the unit of blood, the data corresponding to biometric data;

reading biometric data from the patient; and

blocking transfer of blood from the unit to the patient when the stored data do not correlate with the biometric data read from the patient and otherwise permitting transfer of blood from the unit to the patient.

46. The method of claim 45 wherein the act of collecting stored data comprises scanning a bar code on the unit with a bar code reader.

47. The method of claim 45 wherein the act of collecting stored data comprises reading data from a memory in the unit.

48. The method of claim 45 wherein the act of reading biometric data from the patient comprises reading fingerprint data from the patient.

49. The method of claim 45 wherein the act of reading biometric data from the patient comprises reading iris data from the patient.

50. A method for adding medical data to a database comprising:

obtaining medical data and data corresponding to biometric identifiers;

searching a database to determine if one of the records in the database is a matching record that includes biometric data matching the biometric identifiers;

creating a new record including the medical data and the data corresponding to biometric identifiers when no records already present in the database match the biometric identifiers; and

appending the medical data to the matching record when one of the records does match a record present in the database.

51. The method of claim 50 wherein the act of obtaining biometric identifiers comprises obtaining fingerprint data.

52. The method of claim 50 wherein the act of obtaining biometric identifiers comprises obtaining iris data.

53. The method of claim 50 wherein the act of obtaining medical data comprises obtaining medical data describing blood crossmatch compatibility.

54. A method for linking a parent biometrically to natural offspring, comprising:

collecting first biometric data from the parent contemporaneously with birth of the offspring;

collecting second biometric data from the natural offspring after birth of the natural offspring;

linking the first and second biometric data to form a record; and

storing the record in a database.

55. A method for linking at least one individual to a stored computer record comprising:

taking first biometric data;

comparing the first biometric data to a series of stored computer records;

identifying one of the stored computer records that provides a match to the first biometric data;

taking second biometric data;

comparing the second biometric data to the one of the stored computer records that provided a match to the first biometric data;

activating the first signal when the one of the stored computer records does not match the second biometric data; and

activating a second signal when both the first and second biometric data match the one of the stored computer records.

56. The method of claim 55 wherein the act of taking first biometric data comprises taking first biometric data from a first individual.

57. The method of claim 55 wherein the act of taking second biometric data comprises taking second biometric data from a second individual.

58. The method of claim 55 wherein the act of comparing the first biometric data to a series of stored computer records comprises comparing the first biometric data to a series of stored computer records including stored computer records formed by:

taking a first set of biometric data from a prospective mother in the context of delivery of a newborn;

taking a second set of biometric data from the newborn contemporaneously with the birth of the newborn;

linking the first and second sets of biometric data to form a record; and

storing the record in a database.

59. A method of medical billing comprising:

collecting biometric data from a patient;

linking the biometric data with a test result and billing data from a medical test conducted with respect to the patient to form a computer record; and storing the computer record in a database.

60. The method of claim 59, wherein the acts of collecting, linking and storing are carried out by first computers, further comprising:

inputting biometric data from a patient; and

matching the input biometric data to a series of records stored in a database; and, when the input biometric data match a record stored in the database,

displaying billing information describing treatment that has been rendered to the patient; and, when the input biometric data do not match any record stored in the database,

providing a signal indicating that no match has been identified.

61. The method of claim 60, wherein the acts of inputting, displaying and providing are carried out by second computers and the act of inputting is at the patient's request, the method further comprising:

identifying an erroneous billing displayed in the act of displaying.

62. The method of claim 59, wherein the acts of inputting, displaying and providing are carried out by second computers controlled by a health insurance carrier and the act of inputting is at the patient's request, the method further comprising identifying an incorrect billing displayed in the act of displaying.

63. A method of using stored medical data comprising:

inputting biometric data from a patient into a computer;

comparing the input biometric data from the patient to a series of records stored in a database and accessible to the computer to identify a record including data corresponding to the input biometric data; and

determining that it is appropriate to proceed with medical treatment based on the act of comparing.

64. The method of claim 62, further comprising:

appending information describing the medical treatment and billing information to the record identified in the act of comparing to form an augmented record; and

storing the augmented record in the database.

65. A method for managing a blood bank comprising:

collecting data describing suitability of a first prospective blood donor in a first blood donation center;

collecting first biometric data from the first prospective blood donor;

determining a first deferral status when the first prospective donor is unsuitable as a blood donor and should be deferred and determining a second deferral status when there is no indication of a lack of suitability of the first prospective blood donor;

forming a new record including data derived from the first biometric data and the deferral status; and

storing the new record in the database.

66. The method of claim 65, further comprising:

collecting second biometric data from a second prospective blood donor in a second blood donation center;

comparing the second biometric data to stored records in the database to identify a particular record including data corresponding to the second biometric data; and determining the deferral status of the second prospective blood donor from the particular record identified in the act of comparing.

67. The method of claim 65, wherein the act of forming a new record includes forming a new record further comprising a date of the acts of collecting in the first blood donation center.

68. The method of claim 67, further comprising:

collecting second biometric data from a second prospective blood donor in a second blood donation center;

comparing the second biometric data to stored records in the database to identify a particular record including data corresponding to the second biometric data; and determining the deferral status of the second prospective blood donor and a date of formation of the new record from the particular record identified in the act of comparing.

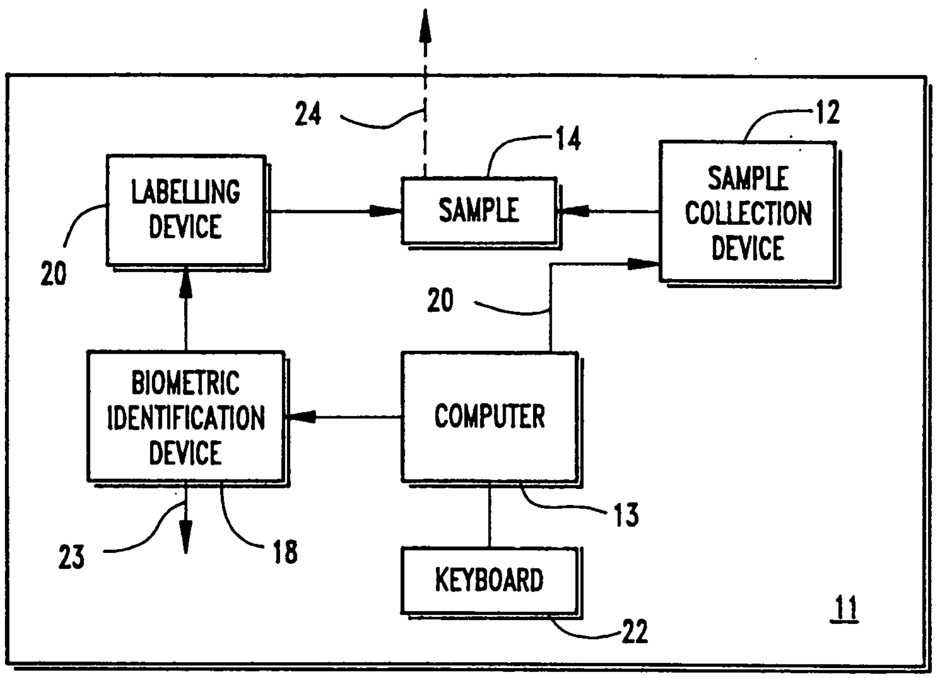

24
LABELLING DEVICE
SAMPLE
14
12
SAMPLE COLLECTION DEVICE
20
20
BIOMETRIC IDENTIFICATION DEVICE
COMPUTER
23
18
13
KEYBOARD
22
11

Fig. 1

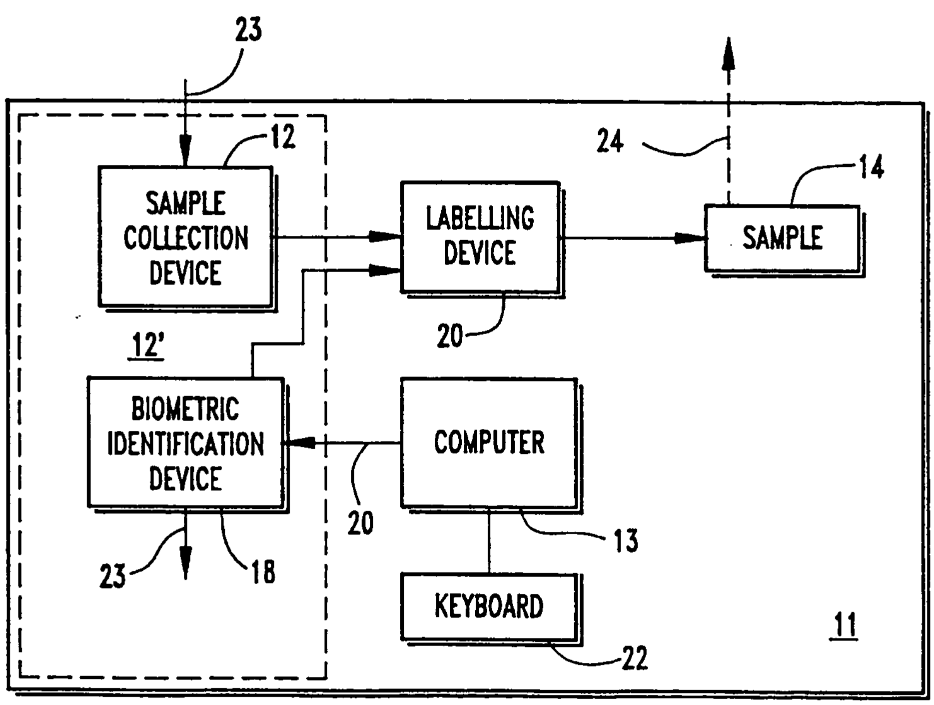

23
24
12
14
SAMPLE COLLECTION DEVICE
LABELLING DEVICE
SAMPLE
20
12'
BIOMETRIC IDENTIFICATION DEVICE
COMPUTER
20
23
18
13
KEYBOARD
22
11

Fig. 2

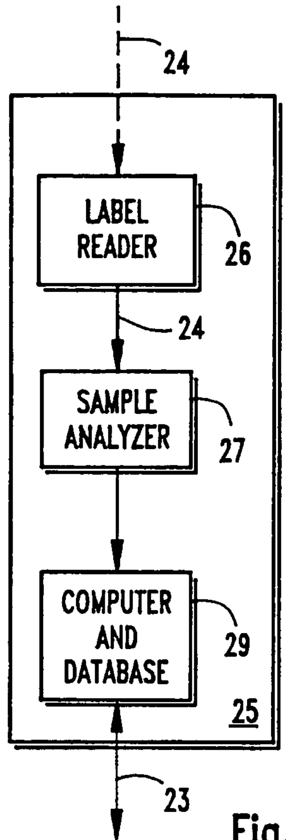


Fig. 3a

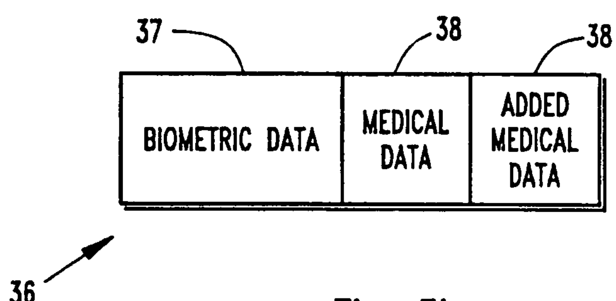


Fig. 3b

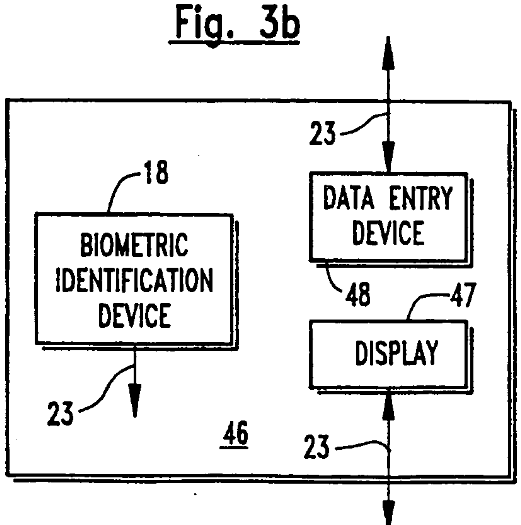


Fig. 6

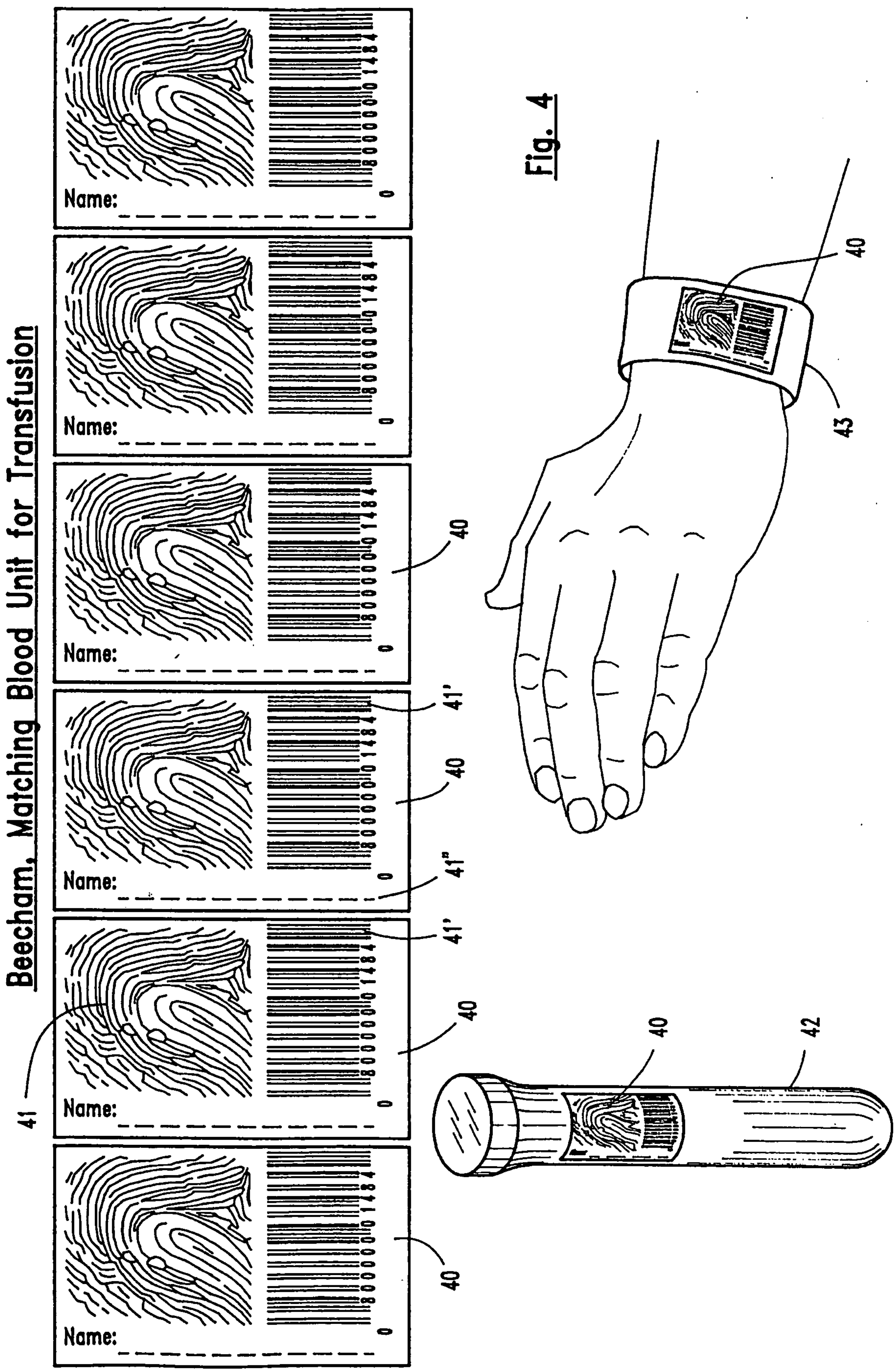

Beecham. Matching Blood Unit for Transfusion
Name:
Name:
Name:
Name:
Name:
Name:
40
41
41'
41"
42
43

Fig. 4

Beecham, Matching Blood Unit for Transfusion

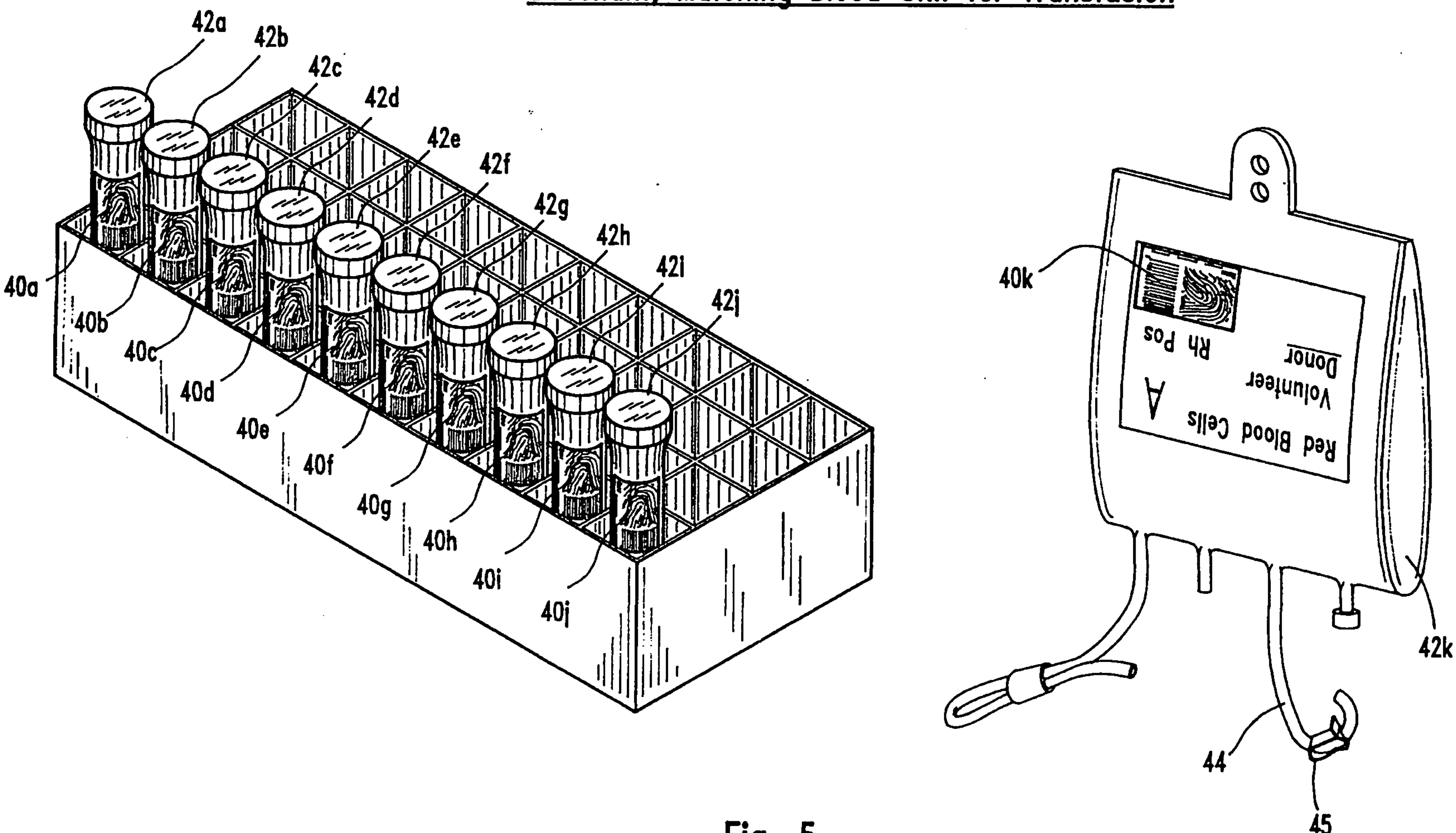


Fig. 5

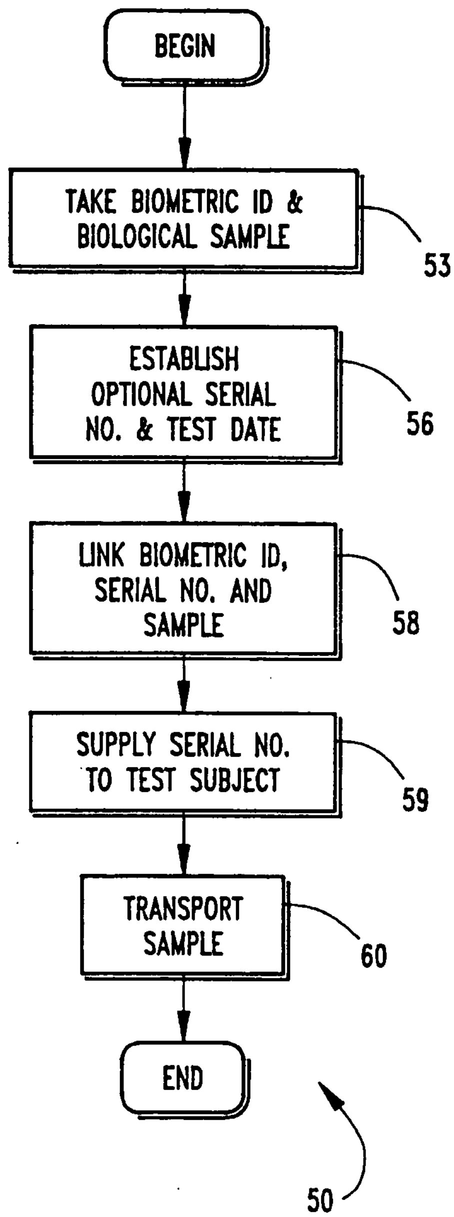

BEGIN
TAKE BIOMETRIC ID & BIOLOGICAL SAMPLE
53
ESTABLISH OPTIONAL SERIAL NO. & TEST DATE
56
LINK BIOMETRIC ID, SERIAL NO. AND SAMPLE
58
SUPPLY SERIAL NO. TO TEST SUBJECT
59
TRANSPORT SAMPLE
60
END
50

Fig. 7

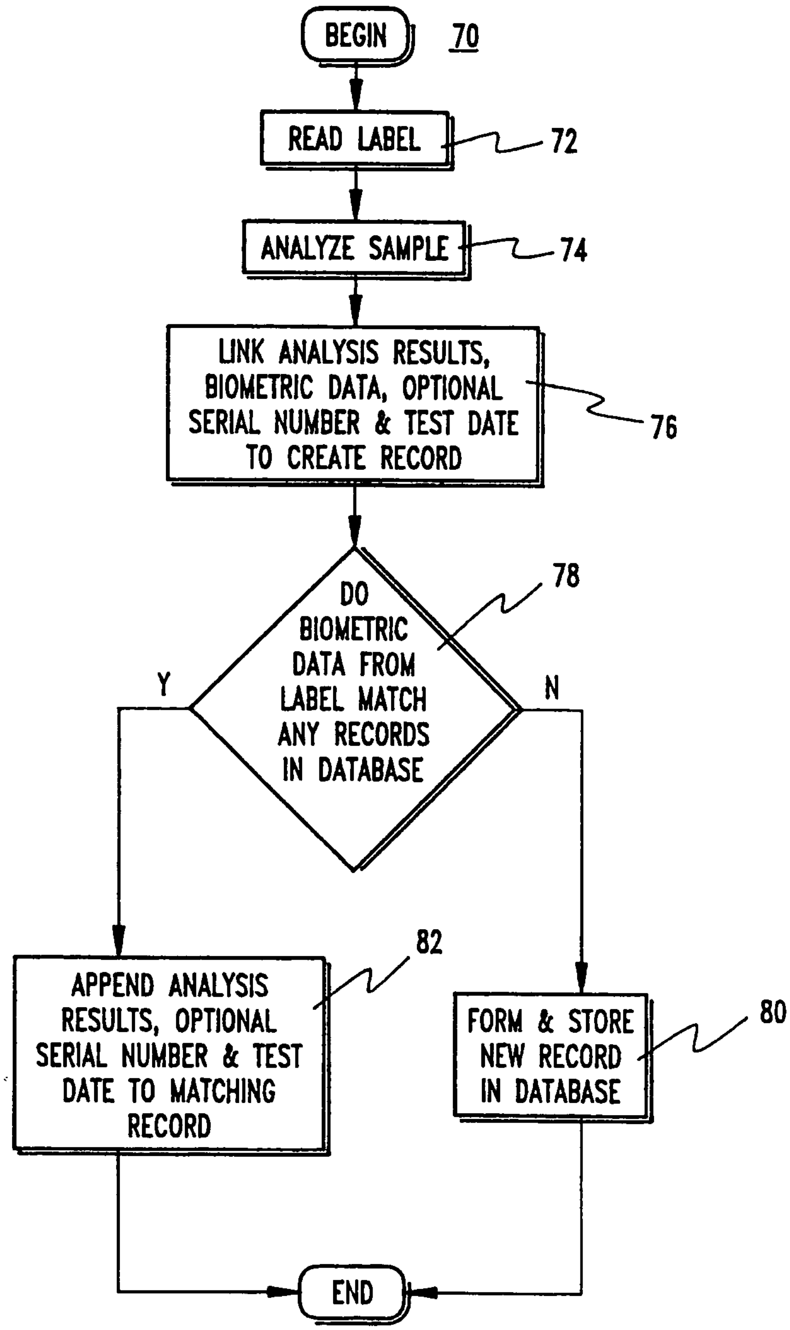

BEGIN
70
READ LABEL
72
ANALYZE SAMPLE
74
LINK ANALYSIS RESULTS, BIOMETRIC DATA, OPTIONAL SERIAL NUMBER & TEST DATE TO CREATE RECORD
76
DO BIOMETRIC DATA FROM LABEL MATCH ANY RECORDS IN DATABASE
78
Y
N
APPEND ANALYSIS RESULTS, OPTIONAL SERIAL NUMBER & TEST DATE TO MATCHING RECORD
82
FORM & STORE NEW RECORD IN DATABASE
80
END

Fig. 8

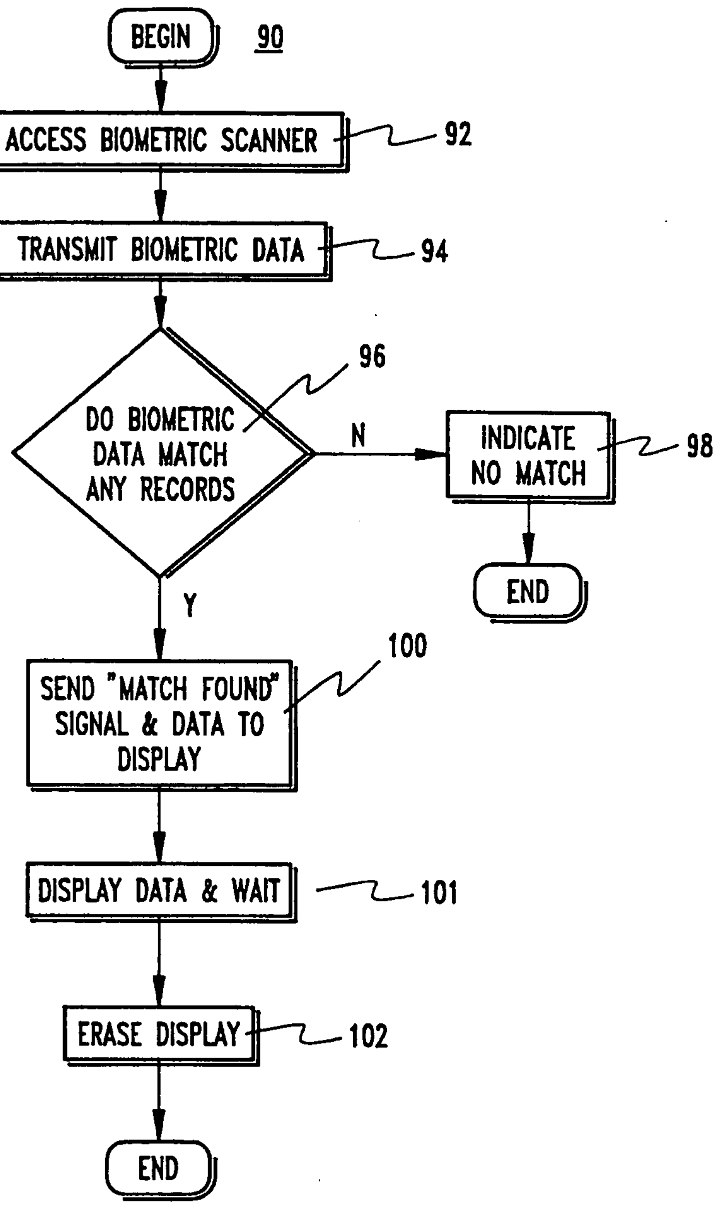

BEGIN
90
ACCESS BIOMETRIC SCANNER
92
TRANSMIT BIOMETRIC DATA
94
96
DO BIOMETRIC DATA MATCH ANY RECORDS
N
INDICATE NO MATCH
98
END
Y
100
SEND "MATCH FOUND" SIGNAL & DATA TO DISPLAY
DISPLAY DATA & WAIT
101
ERASE DISPLAY
102
END

Fig. 9

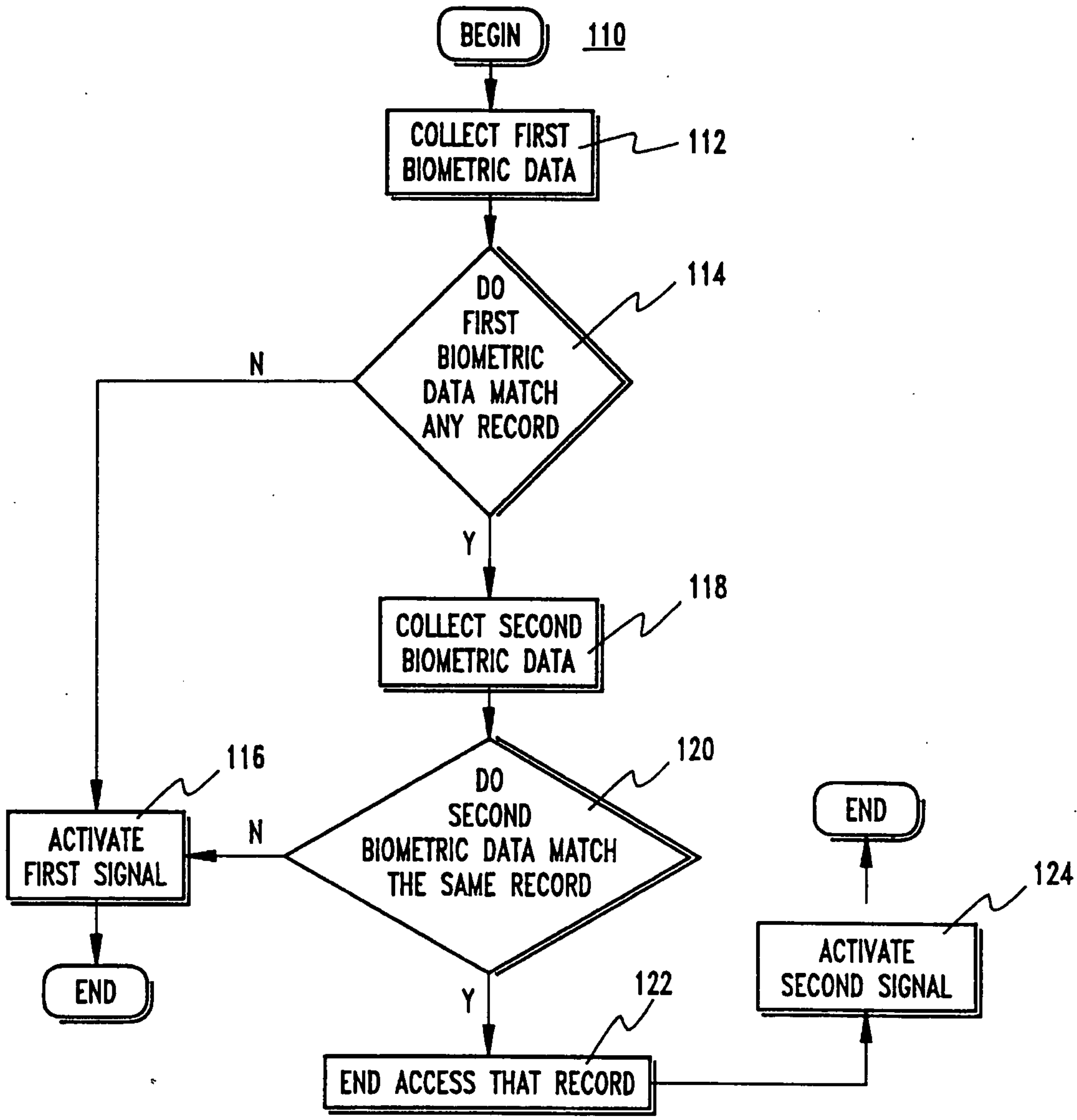

BEGIN
110
COLLECT FIRST BIOMETRIC DATA
112
DO FIRST BIOMETRIC DATA MATCH ANY RECORD
114
N
Y
COLLECT SECOND BIOMETRIC DATA
118
DO SECOND BIOMETRIC DATA MATCH THE SAME RECORD
120
N
Y
ACTIVATE FIRST SIGNAL
116
END
END ACCESS THAT RECORD
122
ACTIVATE SECOND SIGNAL
124
END

Fig. 10

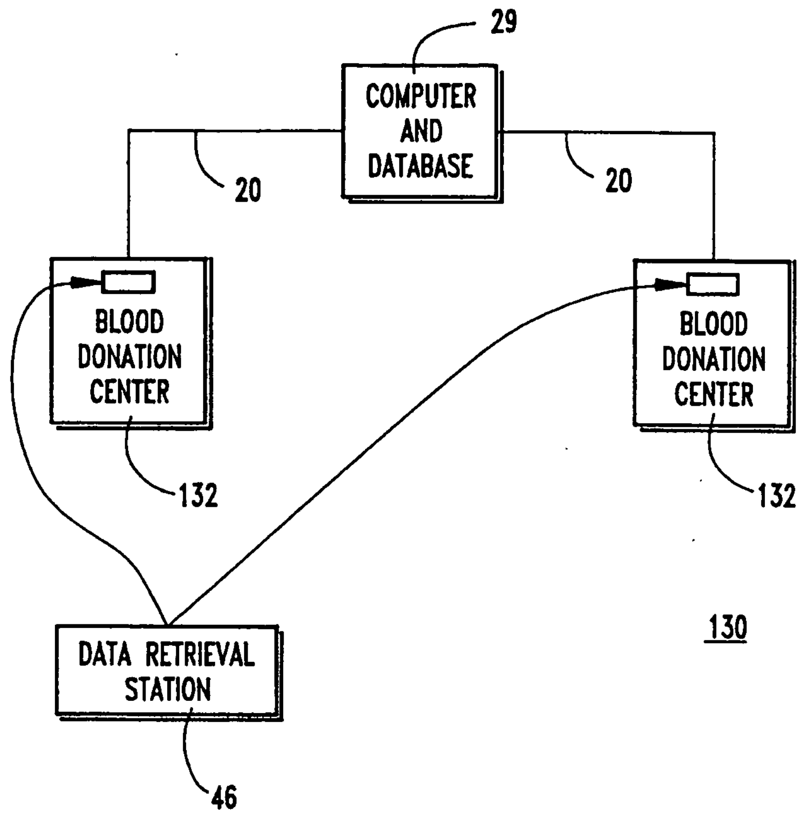

29
COMPUTER AND DATABASE
20
20
BLOOD DONATION CENTER
BLOOD DONATION CENTER
132
132
DATA RETRIEVAL STATION
46
130

Fig. 11

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/20373

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61B5/117

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 02083 A (FINKLER RAMI; SAREL ODED; BAR-ADVANCED CONTROL SYSTEMS LTD) 22 January 1998 (1998-01-22)	1-3
A	page 21, line 24 -page 23, line 4	4-6
X	US 5 719 950 A (ARNESON MICHAEL R ET AL) 17 February 1998 (1998-02-17)	1,2
A	column 5, line 41 -column 7, line 12 column 9, line 51 -column 10, line 49	4-6
X	US 4 449 189 A (FEIX WOLFGANG H ET AL) 15 May 1984 (1984-05-15)	1,5
A	column 3, line 60 -column 4, line 15 column 6, line 46 -column 7, line 8	6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 January 2000	18/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Knüpling, M

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/US 99/20373

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 229 764 A (MATCHETT NOEL D ET AL) 20 July 1993 (1993-07-20)	1,2,5
A	column 6, line 34 - line 62 column 10, line 35 -column 11, line 15 column 11, line 47 - line 49 ---	4,6
A	US 4 993 068 A (PIOSENKA GERALD V ET AL) 12 February 1991 (1991-02-12) column 3, line 66 -column 4, line 16 column 5, line 20 - line 51 column 8, line 33 -column 9, line 21 ---	1-6
A	US 4 458 993 A (KEMPF PAUL S) 10 July 1984 (1984-07-10) column 3, line 30 - line 59 column 2, line 7 - line 20 -----	1,2,4

2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 99/20373

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 7-68
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

see further information sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 7-68

In view of the large number of independent claims (18) and their very different subject-maters by nature (e.g. biometric systems, methods for storing and processing computer records, methods for determining medical treatment) involved in these claims, it is rendered very difficult to analyze with accuracy and without considerable effort the extent and scope of the claims involved. This makes it impossible to clearly identify the invention on which the search ought to be focussed.
In view of the above it was nevertheless decided to carry out a search based on the first independent claim including the claims made dependent thereon.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international sarch report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

..formation on patent family members

Inter nal Application No
PCT/US 99/20373

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9802083	A	22-01-1998	AU 3271397 A	09-02-1998
			CA 2259978 A	22-01-1998
			EP 0929868 A	21-07-1999
US 5719950	A	17-02-1998	AU 2186095 A	09-10-1995
			BR 9507142 A	30-09-1997
			CA 2183886 A	28-09-1995
			DE 69501327 D	05-02-1998
			DE 69501327 T	23-07-1998
			EP 0752143 A	08-01-1997
			ES 2110841 T	16-02-1998
			JP 9510636 T	28-10-1997
			WO 9526013 A	28-09-1995
US 4449189	A	15-05-1984	AT 19588 T	15-05-1986
			CA 1181856 A	29-01-1985
			EP 0082304 A	29-06-1983
			JP 58102300 A	17-06-1983
US 5229764	A	20-07-1993	NONE	
US 4993068	A	12-02-1991	NONE	
US 4458993	A	10-07-1984	NONE	